UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M. FANNO"

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

"Blockchain e cryptovalute: rivoluzione o innovazione?"

RELATORE:

CH.MO PROF. Alberto Lanzavecchia

LAUREANDO: Alberto Pulin

MATRICOLA N. 1114790

ANNO ACCADEMICO 2017 – 2018

INDICE

INTRODUZIONE

Le varie crisi economiche che si sono susseguite negli ultimi anni, e la scarsa fiducia dei risparmiatori nel mercato borsistico e finanziario, hanno portato alla creazione delle cryptovalute. Definite da alcuni come "valute democratiche", dato che la loro emissione non è controllata da enti centrali, sono detenibili in wallet, micro applicazioni apribili in pochi secondi, attraverso le quali è possibile muovere in maniera autonoma la propria liquidità. Queste nuove valute, purtroppo, non stanno registrando una diffusione di massa, poiché molte persone sono scettiche sul loro utilizzo, o sul loro valore futuro, a causa della non materialità delle cryptovalute e della forte volatilità che ne caratterizza il prezzo di mercato (dovuta a illiquidità e, ridotta capitalizzazione del mercato). É da sottolineare però anche la crescita nell'adozione delle cryptovalute soprattutto nei paesi, che stanno soffrendo di altissimi livelli d'inflazione, quali l'Argentina o alcuni paesi Africani, in cui gli abitanti le stanno acquistando per conservare il valore della loro ricchezza, evitando la svalutazione dei propri risparmi, potendole poi convertire immediatamente in base alle necessità, senza richiedere l'intervento di intermediari finanziari, che spesso proprio nei periodi di crisi sistemiche si sono dimostrati insolventi.

Per fare luce su questo nuovo strumento, il mio elaborato presenterà nel primo capitolo delle nozioni teoriche, che servono a comprendere che cosa sono le cryptovalute, come vengono create e come avvengono le transazioni, non chè a sfatare alcuni luoghi comuni che spesso ne limitano il loro utilizzo. Nel secondo capitolo presenterò alcune delle più importanti cryptovalute nel panorama odierno, spiegandone il loro funzionamento ma soprattutto il loro utilizzo o possibili utilizzi negli scambi economici e nella gestione operativa aziendale.

Infine, nell'ultimo capitolo, svolgerò un confronto tra le cryptovalute e internet, due tecnologie simili ma allo stesso tempo diverse che pure stanno modificando profondamente il nostro modo di operare nella quotidianità: sono una rivoluzione o una (formidabile) innovazione?

CAPITOLO 1: Le cryptovalute e la blockchain

1.1 Cosa sono le cryptovalute e brevi cenni storici

Le cryptovalute rappresentano un nuovo sistema di circolazione del denaro e della ricchezza in modo decentralizzato, basato su un sistema di scambio peer-to-peer non controllabile dalle Banche Centrali e nemmeno dagli apparati Statali. La nascita di tale sistema di pagamento risale al 2008-2009[1] con l'invenzione della prima cryptovaluta, che tutt'oggi è la più nota e capitalizzata: il Bitcoin. Questa cryptovaluta viene di fatto anche trattata come valuta di rifugio dagli investitori in tempi di grande volatilità del mercato, o di eventi depressivi o incerti, come i più recenti verificatisi nel mercato.

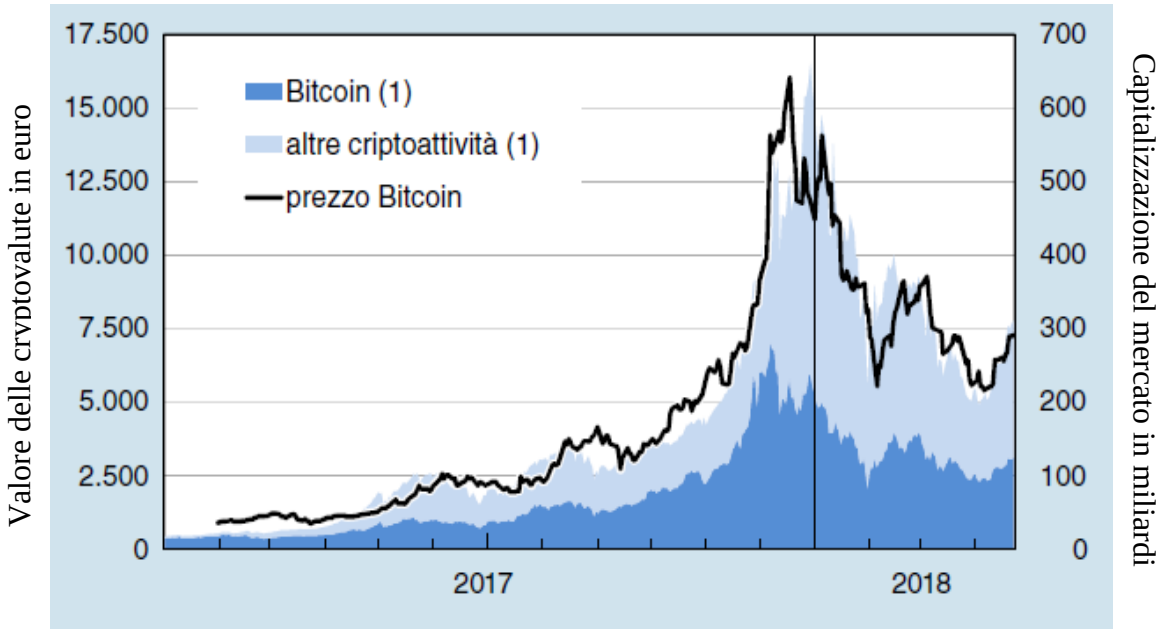


Figura 1: Dominance del Bitcoin rispetto alle altre cryptovalute

Fonte: Rapporto sulla stabilità finanziaria 1 Aprile 2018, prodotto dalla Banca d'Italia in collaborazione con Coinmarketcap

Il Bitcoin è stato creato da Satoshi Nakamoto, nome di fantasia attribuito al suo inventore che deriva da Satoshi l'unità minima della cryptovaluta da lui creata, ed equivalente a 0.00000001 BTC, non essendone stato ancora scoperto il suo vero nome.

Il Bitcoin venne inizialmente creato per trasferire denaro in modo anonimo, grazie a tale anonimità si è creato un gigantesco, per volumi e cifre movimentate, traffico illegale di armi,

[1] Informazione tratta dalle prime pagine di Vincenzo Morabito

droga e merci di ogni genere attraverso la cosiddetta “Silkroad”. La “Silkroad” non era (dato che è stato chiuso) altro che un sito nel “Deep-web” a cui si poteva accedere con protocollo Tor; nonostante la sua chiusura comunque il traffico illegale tramite cryptovaluta permane.
Attualmente la cryptovaluta più utilizzata nel mercato nero per il massimo livello di non tracciabilità è il Monero (XMR).
Nel corso degl’ultimi anni sono state create più di 2000 cryptovalute e il loro utilizzo è molto cambiato, vengono infatti principalmente utilizzate, oltre che per la vendita legale di beni, per prestare servizi online dal settore dei pagamenti al settore medico. La tecnologia sulla quale si basano è chiamata Blockchain che altro non è che:

“*un registro distribuito, non violabile e non modificabile, in una parola 'unhackable', in grado di tenere traccia di qualunque tipo di transazione…*” (Fiorella Cipolletta, 2017).

Si tratta quindi di una nuova tecnologia, basata sostanzialmente su un semplice registro distribuito in rete tramite un’infrastruttura creata attraverso server anche detti nodi che permettono a tutti di conoscere in tempo reale le transazioni avvenute in rete.
Da quanto appena detto sembrerebbe tutto tracciabile, trasparente e riferibile a soggetti definiti ma, in realtà, per operare con le cryptovalute bisogna servirsi di wallet online o hardware che consistono in un conto, simile al conto corrente, dove vengono detenute le cryptovalute, ma, a differenza dello stesso, interamente anonimo. Il numero di conto, infatti, è costituito da numeri e lettere generati automaticamente dal quale non è possibile risalire al soggetto mittente o ricevente, inoltre, ad ogni utilizzo, il numero di conto cambia, anche se il vecchio numero rimane ugualmente funzionante al fine di garantire ulteriore protezione e privacy. Le transazioni, quindi, sono conoscibili da chiunque ma al contempo viene anche garantita la privacy di chi le effettua, il senso di tale sistema è quello di avere un registro delle operazioni in modo da aggiornare i saldi dei vari conti in tempo reale data la sua natura decentralizzata. Il registro, infatti, è fruibile da tutti, ma non modificabile da nessun membro della rete, in quanto è materialmente impossibile modificare tutte le copie di registri decentralizzati contenuti nei vari nodi, o crearne e diffonderne uno falso. In questo modo, si garantisce la non interruzione del servizio, essendo un registro cloud supportato e gestito da moltissimi nodi collegati in rete.
Il funzionamento delle cryptovalute è quindi molto semplice: per inviare denaro, o meglio cryptovaluta, basta conoscere o scannerizzare l’indirizzo di portafoglio di un soggetto o venditore ed inviare un ammontare di cryptovaluta richiesta: un sistema molto semplice e veloce, in quanto, per l’avvenimento della transazione, sono sufficienti pochi secondi e le cryptovalute, a seconda del tipo di utilizzato impiegano al massimo qualche minuto per essere

disponibili nel conto del ricevente. Il tempo per eseguire una transazione però può aumentare, perché essendo la Blockchain una tecnologia trust, necessita di verificare attraverso i vari nodi e il lavoro dei miners che ogni transazione sia corretta, e ogni verifica eseguita prende il nome di confirmation. Nello specifico per ogni confirmation si va ad analizzare che la transazione del mittente sia corrispondente a quella del ricevente attraverso le chiavi pubbliche di entrambi, se ritenuta corretta dalla maggioranza dei nodi la transazione verrà eseguita. La maggior parte dei portafogli online richiede un numero irrisorio di 'confirmations' e quindi la transazione può effettivamente avvenire in pochi minuti anche se le fees sono più elevate, cosa non vera invece per i siti di trading in cui nella maggior parte dei casi per verificare un deposito possono volerci oltre 1000 confirmations e il tempo impiegato è di qualche ora.
Queste sue facoltà sono una novità assoluta in campo economico/monetario poiché facilitano gli scambi di moneta a livello mondiale rendendo veloci, semplici e sicure le transazioni effettuabili anche da smartphone per qualsiasi importo ma, allo stesso tempo, garantendo la non tracciabilità delle stesse: beneficio che possono trarre anche le Banche potendo transare liberamente tra loro in modo anonimo grossi quantitativi di valuta senza renderli visibili e senza bisogno di effettuare richieste a sistemi di controllo o pagare alcun interesse, in modo semplice e soprattutto veloce. Affianco ai benefici, però, ci sono, ovviamente, alcuni problemi che sorgono a causa dell'impossibilità di risalire, con esattezza, a chi ha effettuato una determinata operazione nel mercato: questa incapacità di controllo da parte delle Banche e dello Stato crea il problema di cui parlerò nel corso della mia trattazione, ossia, l'impossibilità di tassazione del "capital gain" generato dal trading sulle stesse, dell'impossibilità di controllare la ricchezza di un soggetto ai fini della tassazione e infine del cosiddetto fenomeno del "money laundering".

1.2 Tipi di cryptovaluta esistenti basati sul sistema di generazione

Esistono principalmente due metodi o meglio, dato che parliamo di valuta virtuale, due protocolli di generazione delle cryptovalute: il POW (Proof of work) e il POS (Proof of stake). Le valute create tramite POW sono la maggioranza di quelle presenti sul mercato a partire proprio dal Bitcoin, la loro generazione avviene tramite il sistema Hashcash introdotto già da Adam Back nel 1997. Il funzionamento di tale sistema è stato spiegato egregiamente da Vincenzo Morabito (2017):

"The hash algorithm then comes up with a complex mathematical computation in which each participating node tries to provide a solution to using the SHA (Secure Hash Algorithm) -256 hash

function. As soon as a solution is provided to the mathematical computation by a node, the particular prerequisites by the proof of work scheme is then thought to be met and this now becomes 'block'."

Ogni cryptovaluta, inoltre, possiede una diversa dimensione fissa per ogni blocco, che altro non è che l'insieme di tutte le transazioni avvenute nell'arco di un certo periodo fino al riempimento dello spazio dello stesso. Quindi ogni cryptovaluta di fatto possiede un determinato tempo per essere, come si dice in gergo, "minata" ossia per portare a termine l'Hash e quindi il calcolo matematico che la trasformerà in un blocco. Tale trasformazione in blocco permette la sua registrazione nella blockchain e la trascrizione definitiva di tutte le transazioni avvenute. Ad esempio, il tempo necessario a minare un blocco del Bitcoin è di 10 minuti, mentre per quello del Monero è di 2 minuti.

Ora è quindi possibile comprendere come viene generata nuova cryptovaluta, infatti, si tratta della ricompensa rispetto al lavoro svolto dai miners per minare l'intero hash del blocco e verificare quindi le transazioni avvenute registrandole in blockchain.

Inoltre, essendo le cryptovalute POW spesso limitate ad un ammontare predefinito prima della loro emissione (es: 21 milioni di BTC totali) la difficoltà, o meglio la ricompensa, per blocco diminuisce con il tempo, infatti, ogni 4 anni, avviene il cosiddetto halving, che aumenta la difficoltà di estrazione di moneta. Questo dovrebbe rendere ad esempio minabile l'ultimo Bitcoin nel 2140, cosa forse difficile perché a quel punto dovrebbe esservi una potenza di calcolo enorme e non ottenibile oggigiorno, quindi dev'esservi anche un progresso nella creazione di sistemi di mining.

È inoltre da precisare che solo colui che risolve il blocco ottiene la ricompensa e quindi se ogni 10 minuti vengono risolti 10 blocchi da 100 persone solo dieci di esse riceveranno una ricompensa che li ripagherà del costo dell'elettricità spesa per minare con il proprio pc o con sistemi più evoluti quali i sistemi Asic. Per questo motivo negl'ultimi anni sono nate le cosiddette mining pools, ovvero, siti che permettono di mettere insieme vari miners e potenza di calcolo in modo da minare più velocemente e più blocchi possibili, dividendo il ricavato in base alla contribuzione di capacità di calcolo fornita da ciascuno misurata in GHZ.

Le valute POS, invece, si sono sviluppate solo ultimamente e per questo sono la minoranza delle cryptovalute oggi esistenti. Esse, come spiega Vincenzo Morabito (2017), sono nate:

"… as an alternative to the proof of work scheme. Proof of stake is a scheme built on less-costly computations. This implies that the proof of stake scheme is not based on costly computations as compared to the proof of work scheme. Rather than depending on the scarce resources (costly computations), the proof of stake scheme is dependent on the entities that hold stake within the

network (this implies a proof of stake holding). In other words, we can say that the resource that the network security is dependent on is the ownership of the coin itself, which implies proof-of-ownership that is also scarce. For the authentication and reception of a transaction to occur (whether fees of transaction or new coins), some of the coin must be owned by a miner. The probability that a miner is successful in the creation of a new block is dependent on the amount of coin owned by the miner and not dependent on the computational power whenever the proof of stake scheme is used."

Questo permette di comprendere che le cryptovalute POS sono nate a causa dell'elevato costo di mining delle cryptovalute POW, la cui tecnica di estrazione chiamata "Stake", non si basa più sulla potenza di calcolo ma bensì sull'ammontare di cryptovaluta già detenuto da ciascun soggetto; Questo meccanismo è molto simile alle azioni, infatti, è come se si detenesse equity e si ricevessero dividendi che vengono tramutati nuovamente in equity posseduta.
Sorgono comunque alcuni problemi in questo sistema di creazione, soprattutto per quanto riguarda la sicurezza poiché il deposito di cryptovaluta dev'essere effettuato in un portafoglio che va lasciato aperto esclusivamente per lo "Stake"[2], quindi non è cifrato e i furti di cryptovaluta sono all'ordine del giorno.
È inoltre da ricordare l'ultima formazione di cryptovalute ibride POW/POS, la cui capofila ad utilizzare tale protocollo, anche se precedentemente era una valuta POW, è l'Ethereum.
Affianco ai sistemi classici di creazione se ne affacciano altri meno consolidati, ma ugualmente funzionali, primo fra tutti il nuovo sistema ideato da PO.et che si basa su un sistema di Proof of existence e che mira ad essere utilizzato per verificare l'autenticità digitale; Il tutto viene realizzato con un market e con la possibilità di vendere scritti così da creare una sorta di immensa biblioteca al fine di utilizzarla per verificare l'autenticità di ogni scritto in rete.

1.3 Differenze tra le cryptovalute e la moneta

Da quanto detto sopra è intuibile che vi sono delle differenze tra le cryptovalute e la moneta che usiamo tutti i giorni per le transazioni. Le principali differenze tra questi due sistemi di pagamento sono le seguenti [3]:

1) La mancanza di un ente centrale di emissione, infatti la creazione di nuova cryptovaluta è decentralizzata e basata su un sistema di ricompense ossia, come si dice in gergo

[2] Lo Stake è il sistema utilizzato per minare le cryptovalute POS e consiste nel detenere le medesime in un conto aperto, maggiore è la quantità in conto, maggiore sarà la probabilità di minare nuova valuta.
[3] Maggiori differenze sono rinvenibili nell'articolo di Sarah Rotman Parker (2014) da cui ho preso uno spunto per tale riflessione

provata dal lavoro svolto o al massimo dallo stake di cryptovaluta eseguito. A questo è dovuta anche la non materialità delle cryptovalute, poiché esistenti solamente in formato digitale e non materializzabile. Quanto appena detto non è del tutto esatto in quanto è possibile utilizzare monete dotate di microchip o i paper wallet, anche se non paragonabili alle monete o banconote coniate da un Istituto centrale quali le Zecche o la Banca Centrale Europea.

2) L'anonimità dei trasferimenti che è stata lo scopo principale della loro creazione, garantita grazie ad un adress di portafoglio generato automaticamente e senza alcun collegamento con il soggetto detentore.

3) La non inflazionarietà delle cryptovalute, perché generalmente sono limitate nel valore di emissione, vi sono però anche cryptovalute che aumentano la base circolante come l'Ethereum. L'aumento della sua base monetaria è di circa un 3% annuo prestando attenzione alla condizione di domanda e offerta in modo da non svalutarla, valore che riporta alle teorie Monetariste del primo '900.

I monetaristi guidati da Fisher furono tra l'altro portatori di una innovativa teoria volta a spiegare il collegamento tra la quantità di moneta in circolazione e il livello d'inflazione; Tale teoria, denominata "la teoria quantitativa della moneta" è espressa dalla seguente formula:

$$M \times V = P \times Y$$

- M=quantità di moneta
- V= velocità di trasferimento
- P=prezzi
- Y=reddito=beni prodotti nell'anno

In particolar modo tali studiosi sostenevano che né la velocità di trasferimento né il reddito potessero cambiare nel breve e quindi che un aumento di della quantità di moneta, avrebbe portato ad un aumento dei prezzi; proprio per questo motivo ritenevano necessario un aumento contenuto della quantità di moneta in circolazione stimato nel range dal 3% al 5% annuo, per evitare l'eccessivo aumento dei prezzi che avrebbe causato inflazione.
Tali percentuali erano basate su una normale crescita del PIL e quindi del Reddito calcolata statisticamente nel corso degli anni passati; erano inoltre convinti della non incidenza di una politica fiscale sul tasso d'interesse.

Questa teoria fu ribadita e modificata dai Keynesiani, i quali sostenevano che anche nel breve vi potesse essere una variazione della velocità di trasferimento e del reddito e che fosse plausibile un'influenza della politica fiscale attraverso il famoso moltiplicatore del reddito.
La formula della circolazione monetaria fu modificata in:

$$M=PKY$$

- M=quantità di moneta
- K= %di reddito detenuta e non circolata (Può essere visto come il reciproco di V)
- P=prezzi
- Y=reddito=beni prodotti nell'anno

Quindi sostanzialmente quest'ultimi affermarono che, anche se la quantità di moneta in circolazione dovesse aumentare, non si avrebbe un aumento dei prezzi se la circolazione della moneta fosse più lenta a causa di investimenti o per altri usi.
Ho fatto tale parentesi macroeconomica per spiegare l'ultima differenza tra le cryptovalute e la moneta che ritengo essere rilevante, ossia la maggiore velocità di trasferimento delle cryptovalute rispetto agli odierni sistemi di pagamento che, come affermato in precedenza e come sostenuto anche da Pedro Franco (2015):

"this could lead to an increase in the velocity of fiat currencies[4], as the need to hold fiat currencies would decrease. Such an increase in the velocity of money could lead to inflation, forcing central banks to decrease the money supply, i.e.implement a tightening of the monetary policy."

Quindi si rende necessario l'intervento da parte della Banca centrale Europea, ma in generale di tutte le Banche centrali mondiali che possono incidere attraverso i loro poteri sulla politica monetaria al fine di evitare che la diminuzione di K possa portare ad un aumento dei prezzi.

$$\uparrow P = \frac{M}{KY\downarrow} \uparrow$$

Tale intervento deve concretizzarsi in una politica monetaria restrittiva, in modo da ridurre la quantità di moneta in circolazione, evitando che (1/K=V) la maggiore velocità delle transazioni porti ad un aumento nel livello dei prezzi.
In realtà non verrebbe ridotta la base monetaria ma si andrebbe a compiere una vera e propria sostituzione monetaria, intervento che è auspicato da tutti coloro che operano già in questo mondo/settore.

[4] Per fiat currency si fa riferimento alla moneta legale con circolazione forzosa nei vari paesi.

1.4 Differenze tra le cryptovalute e le monete complementari

Le cryptovalute sono diverse anche dalle cosiddette monete complementari, in quanto quest'ultime non vengono create attraverso computer, Asic, o acquistate con la moneta a corso forzoso ma bensì si possono ottenere tramite la vendita dei propri prodotti all'interno di un circuito precostituito. Un'altra caratteristica che le contraddistingue è la non convertibilità in valuta fiat, e quindi il solo utilizzo all'interno del circuito.
Questi circuiti sono utili agli imprenditori al fine di permettergli di vendere la parte di fatturato che non ha domanda in moneta avente corso forzoso, e per questo possono aderire a tale circuito in modo da vendere l'intero fatturato o aumentare la produzione spingendola fino al punto di ottimo tecnico/ economico. La vendita di tali prodotti, permette di ottenere moneta complementare spendibile solo acquistando prodotti di altri venditori del circuito, è inoltre stimata, che tale moneta complementare, essendo forse meno sicura rispetto alla moneta avente corso legale circola con una velocità maggiore dell'ordine di 10X . La maggiore velocità di circolazione del denaro porta ad un aumento scambi e ripresa dell'economia locale, dato che i circuiti sono costruiti su base regionale. In Italia sono presenti realtà già consolidate come il Sardex in Sardegna, il Tibex in Lazio e in Veneto nel 2016 è partito anche il Venetex. Da quanto detto risulta lampante la differenza tra le cryptovalute e le monete complementari in quanto le prime mirano a sostituire le valute fiat nell'uso quotidiano semplificando, velocizzando, rendendo più sicuri i pagamenti e offrendo nuovi servizi, mentre le valute complementari sono circoscritte nel territorio, ambendo ad un'esigenza puramente imprenditoriale comunque molto importante.

1.5 Falsi problemi delle cryptovalute pompati dalle news

"Il Bitcoin e le cryptovalute sono una catastrofe ecologica "

Questo è uno dei titoli enfatizzanti che circolano in alcune testate giornalistiche o blog in rete ed è un segnale di allarmismo riguardo all'elevato consumo energetico usato per la loro creazione. Non miro e non è mia intenzione negare l'evidenza di un problema che effettivamente permane nonostante alcuni tentativi siano stati fatti per ridurne il consumo energetico. Infatti come detto in precedenza, alcune cryptovalute hanno cambiato la modalità di generazione passando dai sistemi POW più energy intensive, ai sistemi POS o addirittura ibridi che consumano meno elettricità per la loro creazione. Il problema però non risulta essere

reale in quanto secondo alcuni studi di Marc Bevand resi poi noti da Bloomberg in un articolo scritto da Elanie OU nel 2017 si dice che:

"A recent report suggests that at current prices, Bitcoin miners will consume an estimated 8.27 terawatt-hours per year. That might sound like a lot, but it's actually less than an eighth of what U.S. data centers use, and only about 0.21 percent of total U.S. consumption. It also compares favorably to the currencies and commodities that bitcoin could help replace: Global production of cash and coins consumes an estimated 11 terawatt-hours per year, while gold mining burns the equivalent of 132 terawatt-hours. And that doesn't include armored trucks, bank vaults, security systems and such. So in the right context, bitcoin is positively green."

Quindi converrebbe sostanzialmente minare e creare valuta digitale rispetto a produrre le monete e le banconote oggi usate. Si potrebbe inoltre risparmiare l'energia per estrarre l'oro in quanto anche se non tangibile il bitcoin è già stato paragonato ad una riserva di valore come l'oro grazie alla sua non inflazionarietà e difficoltà di estrazione. E' da notare inoltre che il suo valore ha superato largamente il valore dell'oro all'oncia essendo oggi pari a circa 8000€ il Btc. Le altre cryptovalute oltre che per gli scambi monetari possono essere viste come una sorta di equity delle società che le hanno emesse, dato che alla fondazione di una nuova altcoin ne vengono distribuite alcune in cambio di fondi, comunque approfondirò meglio più avanti questo argomento quando spiegherò cos'è una ICO.
Tuttavia, se le banche centrali non inizieranno ad accettare le cryptovalute e continueranno a combatterle, si rischia di sprecare ingenti quantità di elettricità, per creare delle valute digitali prive di alcun senso e valore. È per questo motivo che molti sostengono che non siano altro che una bolla speculativa, non capendo esattamente come vengono create e la difficoltà che si ha per estrarre tali cryptovalute dovuta all'enorme potenza di calcolo necessaria e misurabile in ingenti costi sia per i sistemi di minaggio che di elettricità. Questa lotta delle Banche Centrali, secondo quanto già detto, è priva di ogni significato poiché le cryptovalute sono inarrestabili data la loro anonimità e non rintracciabili da nessun ente centralizzato, ma allo stesso tempo possono essere spostate in pochi secondi da un capo all'altro del mondo con un semplice click.
Un secondo problema di cui ci tenevo parlare è il cosiddetto fenomeno del money laundering anch'esso molto discusso in rete, ed usato principalmente per infangare le cryptovalute, senza alcun effettivo fondamento pratico e teorico. Per money laundering innanzi tutto si intende il funzionamento delle cryptovalute come sistema per il lavaggio di denaro sporco da parte di criminalità organizzate. Avevo già accennato all'uso delle cryptovalute sin dalla loro ideazione per il traffico illegale, e quindi non voglio negarne l'evidenza ma rispetto al riciclaggio

mondiale stiamo parlando di numeri molto esigui come evidenziato dallo studio condotto da Elliptic (Fondazione di prevenzione, ricerca e punizione di illeciti finanziari e criminali attraverso le cryptovalute) del 2018 che ha evidenziato i seguenti dati:

Tab.1

ORIGIN OF ILLICIT BITCOINS ENTERING CONVERSIONS SERVICES: LARGEST SOURCES					
Name	2013	2014	2015	2016	All Years
Abraxas	-	0.00%	8.99%	-	3.00%
Agora	0.02%	42.43%	47.89%	0.05%	26.30%
AlphaBay	-	0.00%	9.38%	46.65%	6.26%
Evolution	-	8.35%	10.09%	-	5.40%
Middle Earth Market-place	-	0.05%	5.59%	-	1.88%
Nucleus Market	-	0.01%	13.6%	31.21%	6.63%
Sheep Marketplace	8.42%	-	-	-	3.00%
Silk Road	89.89%	-	-	-	32.03%
Silk Road 2.0	1.03%	40.50%	-	-	10.21%
Total	99.37%	91.35%	95.54%	77.92%	94.70%

Tab.2

PERCENTAGE OF ALL INCOMING TRANSACTION VOLUME ORIGINATING FROM ILLICIT ENTITIES, BY CONVERSION SERVICE TYPE					
	2013	2014	2015	2016	All years
ATM	-	0.07%	0.02%	0.02%	0.02%
Bitcoin Exchange	1.01%	0.37%	0.34%	0.09%	0.37%
Crypto-Exchange	0.17%	0.06%	0.09%	0.00%	0.04%
Gambling	0.69%	3.76%	3.58%	0.57%	2.01%
Mixer	22.57%	29.26%	24.07%	2.81%	16.03%
Multi-Service	0.15%	0.45%	0.46%	0.06%	0.28%
Grand Total	1.07%	1.04%	0.64%	0.12%	0.61%

Tabella1-Tabella2: Dati indicativi sul commercio illegale tramite cryptovaluta
Fonte: https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf?t=1525001933973

La tabella 1, in particolare mostra il traffico di denaro sporco nelle grandi piattaforme del Deep Web, tra le quali la più utilizzata a tale scopo come già sostenuto fu la prima creata, ossia la "Silk Road" attualmente chiusa dalle autorità Statali.

A seguito di tale chiusura, come da tabella si evidenzia uno spostamento di massa su Nucleas Market e AlphaBay. Nel corso del 2017 si è registrata inoltre, la chiusura di Nucleas Market e molto probabilmente vi è stato uno spostamento su AlphaBay che detiene oggi le maggiori quote di traffico illegale a cui fa seguito Dream Market.

La Tabella 2 però ci fornisce un ulteriore dato interessante a confermare la marginalità del traffico illegale tramite cryptovalute, che ha subito una decrescita esponenziale nel corso degl'anni. Considerando le più di 300000 transazioni al giorno solamente del Bitcoin, uno 0,12% di traffico illegale rispetto al totale degli scambi, è un dato marginale e si può quindi considerare tale traffico inesistente. È anche vero però che il Bitcoin risulta essere meno usato a tal fine, infatti le monete oggi preferite a ciò sono, come già dicevo: il Monero o lo Zcash. In ogni caso, essendo le piattaforme le medesime di quelle indicate in Tabella 1 si evince una decrescita e quindi il trend di Tabella 2 è confermato in decrescita.

1.6 Uno sguardo alle cryptovalute come sistemi di investimento

Le cryptovalute oltre che come sistema di pagamento come tutte le valute del mondo, possono essere usate anche per fini di investimento. Esistono infatti siti di trading molto più accessibili e pratici rispetto ai siti di trading tradizionali con commissioni enormemente inferiori in cui è possibile effettuare scambi tra la valuta corrente e le principali cryptovalute e, successivamente, poi tra le medesime e altre cryptovalute minori. Non si tratta di trading di futures o di altri

strumenti derivati, ma di vero e proprio scambio di valuta che è una cosa stravolgente non possibile nel mondo finanziario regolamentato. Forse può sembrare difficile da comprendere ma è molto semplice: si tratta di uno scambio con commissioni che variano dallo 0,01% allo 0,04% di cryptovaluta con altra, potendole poi prelevare o riscambiare all'occorrenza.

Questa cosa non è possibile nel mercato regolamentato perché non è ancora stata inventata una carta/conto corrente forse per interessi bancari, che possa detenere in maniera separata molte valute contemporaneamente lasciando all'utente la decisione di quale utilizzare. Un'altra cosa stravolgente e innovativa, fondamentale nel trading di cryptovaluta consiste nell'esistenza delle "API KEY", si tratta di semplici chiavi di accesso al conto di trading, personalizzabili in base alle operazioni eseguibili che permettono di collegare il proprio conto con delle App per smartphone per operare in multipiattaforma evitando di accedere ogni volta al conto di trading, rimanendovisi sempre collegati e potendo operare con strumenti anche aggiuntivi ad esso.

Le cryptovalute aprono quindi le porte ad un altro modo di fare trading, molto più semplice, veloce e a portata di mano ma soprattutto accessibile a tutti. Ritengo, infatti, che la facile accessibilità sia fondamentale per permettere a tutti di essere liberi di investire senza intermediari e senza grosse difficoltà, cosa che risulta invece difficile nel mercato regolamentato dove, a seguito di una semplice ricerca online risultano molti di siti di trading poco affidabili, con elevate commissioni e pochi strumenti, cosa inaccettabile essendo un mercato regolamentato per cui sarebbe d'obbligo un controllo su Internet. A seguito di ciò sembra quasi che si sia obbligati a rivolgersi presso un intermediario, date anche le difficoltà esistenti in materia di tassazione.

Queste difficoltà in materia di tassazione non sorgono per quanto riguarda le cryptovalute e anche per le valute estere se non si usassero derivati, entro i limiti stabiliti dalla risoluzione n° 72/ E pubblicata dall'Agenzia delle entrate che paragona il Bitcoin e, in generale, tutte le cryptovalute, alle valute estere. Si stabilisce quindi che non è applicabile alcuna tassazione sul reddito derivante dalle plusvalenze dall'attività di trading, entro una certa soglia massima che si configura in 51.645,69€ di giacenza per più di sette giorni consecutivi nei conti di tutti gli intermediari utilizzati. Quindi per la classe media di fatto è possibile investire tranquillamente nelle cryptovalute e senza alcuna tassazione sui profitti generati da tale attività.

Esiste però, in questo mercato, un'elevata volatilità che comporta, ovviamente, elevata deviazione standard e quindi un maggiore rischio di investimento, ciò è ritenuto un fattore conveniente per alcuni ma svantaggioso per altri

$$\sigma i = \sqrt{\frac{\sum_{i=1}^{n}(R-\overline{R})^2}{n-1}}$$

Un tale livello di volatilità non è presente in nessun mercato regolamentato, ed è una cosa positiva per avere un portafoglio più performante cercando allo stesso tempo di limitare il rischio con altri investimenti correlati negativamente ad esso. Per elevata volatilità intendo modifiche del prezzo giornaliero anche di un 10-20% e in casi straordinari, ma nemmeno troppo del 100%. È quasi impossibile limitare il rischio di portafoglio operando nel solo mercato delle cryptovalute perché, come già mostrato dalla *fig.1* all'inizio della mia trattazione, che cerca di dare un quadro d'insieme, la dominance del Bitcoin è molto elevata essendo una cryptovaluta che tutti prendono in considerazione, anche se ultimamente in maniera meno forte rispetto al passato, e il suo andamento rappresenta il trend del mercato in generale.

Tale trend è sicuramente confermato in periodi di flessione negativa, periodi nei quali dovrebbe entrare in gioco la diversificazione del portafoglio per limitare le perdite ma ciò non avviene, in tali periodi, infatti, la dominance del Bitcoin aumenta, provocando a sua volta, l'aumento della sua capitalizzazione / domanda limitandone il trend negativo, mentre le altre cryptovalute riducendosi enormemente la domanda sovraperformano negativamente, salvo casi di speculazione su cryptovalute poco capitalizzate.

Quindi possiamo affermare che vi sia una correlazione delle cryptovalute rispetto al Bitcoin molto forte con p (indice di correlazione) > 0 e, per alcune con un $\beta>1$ ossia con andamento sovraperformante rispetto al Bitcoin, per altre con $\beta<0$ sottoperformanti rispetto ad esso.

A confermare quanto da me sostenuto è uno studio di Vasily Sumanov, pubblicato su Cointelegraph, che è un famoso blog sulle cryptovalute, in cui mette a confronto tre delle più note cryptovalute, e il risultato è la seguente matrice:

CORRELATION MATRIX

	BTC	ETH	LTC	XRP
BTC	1			
ETH	1	1		
LTC	0.93453994	1	1	
XRP	0.729007266	1	0.89282622	1

Figura 2: Correlazione tra le principali cryptovalute
Fonte: https://cointelegraph.com/news/how-to-diversify-away-risk-in-a-crypto-portfolio-correlation-and-variance

Dopo quanto detto dovrebbe essere chiara la presenza di un elevato rischio nell' effettuare un investimento a medio/ lungo termine, come anche a breve in tale mercato. Il problema sorge

soprattutto a causa delle grosse speculazioni che vi sono in tutti i mercati, anche in quelli regolamentati, però in questo caso essendovi una minore capitalizzazione/ liquidità un aumento inferiore della medesima può far salire repentinamente il prezzo, parliamo infatti per tale mercato di una liquidità pari allo 0,5% di quella del mercato finanziario odierno come analizzato dall'articolo di Repubblica (Aprile 2018) che critica inoltre le cryptovalute definendole una bolla speculativa in cui l'investimento è trainato dalla la ricerca di profitto. Evento emblematico di tale speculazione si è avuto a metà Settembre scorso quando Jamie Dimon (CEO di JPMorgan) in un famoso articolo pubblicato inizialmente da Reuters (Settembre 2017) e poi diffusosi in tutta la rete dichiarava, già in un momento non felice per il mondo delle cryptovalute, dato il Ban proclamato e mai verificatosi in Cina che il Bitcoin non era altro che una truffa. Questo portò come da immagine sottostante al verificarsi di un crollo del Bitcoin, ma anche delle altre cryptovalute:

Figura 3: Grafico del Bitcoin
Fonte: www.Coinmarketcap.com

In questo caso si trattava di un mero evento speculativo infatti lo stesso Jamie Dimon acquistò Etf del Bitcoin, titoli del mercato regolamentato che replicano l'andamento del sottostante (in questo caso il Bitcoin), per 3 milioni di euro non prima di averne ridotto il prezzo, tale azione oltre che essere illegale rientrando nella fattispecie dell'aggiotaggio, prova anche la falsità della notizia fatta passare giorni prima.

A testimoniare l'incongruenza totale di tale agire fu la dichiarazione, fatta da Nikolaos Panigirtzoglou, esperto di global market in JPMorgan, pubblicata da CNBC (Dicembre 2017) in cui smentisce quanto detto a Settembre dal proprio CEO, sostenendo che la creazione dei futures sul Bitcoin potrebbe fornire maggiore legittimità alle cryptovalute aumentandone l'appeal sul mercato, soprattutto per grossi investitori istituzionali.

Concludendo quanto detto, ritengo che il mondo delle cryptovalute possa avvicinare molte persone al trading, ma allo stesso tempo non nego la possibilità che vi sia una vera e propria

bolla speculativa, cosa non diversa del mercato regolamentato, ma il concetto che voglio ribadire con la mia tesi, non è tanto l'importanza delle cryptovalute in quanto mero strumento d'investimento, bensì dell'innovazione che tali cryptovalute stanno portando cambiando in modo positivo e innovativo il nostro futuro, mettendo a disposizione una serie di servizi e banche dati disponibili a tutti in ogni momento.

CAPITOLO 2: Alcune Cryptovalute e soluzioni innovative apportate

2.1 Ethereum: Dapps e Smart contracts

Una delle valute più innovative e importanti create dopo la nascita del Bitcoin è Ethereum, infatti si tratta della seconda cryptovaluta per capitalizzazione di mercato, in grado oltre che di essere usata come mezzo di pagamento, anche di offrire servizi per l'intero mondo delle cryptovalute. La sua nascita risale solamente all'Agosto 2015 quando il suo inventore, un programmatore Russo di nome Vitalik Buterin, creò Ether vero nome della cryptovaluta che successivamente è stato snaturato. La sua idea fu rivoluzionaria rispetto alle valute precedenti che si affiancavano al Bitcoin senza alcuna novità, se non per leggere variazioni nei protocolli di trasferimento (eccetto Litecoin che puntava, e nel 2017 è riuscito grazie al Lightning Network[5] ad essere l'argento digitale e sussidiario del Bitcoin), Ethereum invece si distinse subito da tutte le altre cyptovalute in quanto fu creata per fornire molti servizi tra i quali la possibilità di svolgere crowdfunding di progetti basati sulla propria piattaforma, di sostenere altre cryptovalute basate sulla propria blockchain, e la possibilità, inoltre, di essere usata come piattaforma Dapps, ma la novità che l'ha resa celebre è stata l'ideazione degli Smart Contracts. Per quanto riguarda la sua peculiarità come piattaforma Dapps, essendo stata la prima ad essere creata, annovera secondo i dati di Dappradar (servizio che analizza le Dapps esistenti) circa 500

[5] Il Lightning Network consiste in una modifica importante nel protocollo di trasmissione del Litecoin, consentendo a tale cryptovaluta di essere convertita immediatamente in Bitcoin se inviata ad un adress corrispondente ad un wallet Bitcoin. Grazie al Lightening network, Litecoin raggiunse il valore attuale, diventando di fatto l'argento digitale e allo stesso tempo risolvendo il problema principe del Bitcoin ovvero le alte fees che non consentono transazioni per importi irrisori e soprattutto risolvendo importanti problemi di scalabilità. La cryptovaluta che sarà la più scalabile secondo il mio punto di vista sarà in grado di diventare la nuova moneta sbaragliando completamente tutta la concorrenza, infatti tutti puntano a creare o migliorare la propria cryptovaluta renderla più scalabile possibile, ma per ora nessuna è riuscita ad esserlo a livelli tali per essere moneta e infatti parliamo di cryptovalute.

Dapps, ma sicuramente la più nota dato che mandò in sovraccarico il sistema per il numero di transazioni effettuate in Ethereum a inizio Dicembre scorso, è CryptoKitty. Si stimò in tale occasione (Bloomberg, 4 Dicembre 2017), che fossero stati spesi in meno di 24h, Ethereum per un controvalore di 3 milioni di euro al fine di acquistare dei gattini.

Le Dapps non sono altro che applicazioni per pc o smartphone basate sulla tecnologia di trasmissione P2P[6], non tutte ovviamente si basano sulla blockchain, ed è bene fare chiarezza per evitare fraintendimenti. Esistono infatti Dapps basate sul protocollo P2P, nate anche prima della blockchain stessa che non hanno nulla a che fare con essa: faccio riferimento ai sistemi di download tramite Torrent e il famoso sistema Tor, che riescono a diffondersi talvolta anche illegalmente (nonostante le varie cause legali in atto), in quanto risulta difficile eliminare tale traffico perché poggiano su un sistema decentralizzato.

Per entrambi i tipi di applicazioni, infatti, la decentralizzazione è un fattore critico di successo, che permette alle Dapps basate su blockchain di essere molto più rapide nell'esecuzione, di evitare eventuali problemi di aggiornamento (basta il consenso della maggioranza dei membri del network), e di superare eventuali sovraccarichi di sistema (ogni computer che la utilizza diventa di fatto un nodo espandendo il network). La decentralizzazione comporta però, a sua volta, la necessità di criptare le varie informazioni degli utenti per evitare la fruizione dei dati personali da parte della community che le utilizza, a questo scopo nascono dei token per ripagare il lavoro dei miner, che stavolta non fanno altro che criptare e registrare le informazioni raccolte da ogni singolo utente. L'accesso alle Dapps non avviene come per le App normali attraverso un form di frotntend (che comunica con una Api, connettendosi poi ad un Database e passando le varie informazioni), perché data la vastità dei nodi sarebbe impossibile.

Quindi per le Dapps, si è sviluppato un nuovo metodo di connessione attraverso gli Smart Contracts. Per accedere all'applicazione è dunque richiesto l'acquisto tramite token, in questo caso Ethereum, di uno Smart Contract che rappresenta una sorta di licenza d'uso attraverso la quale è possibile interfacciarsi con applicazioni di tipo decentralizzato. Ethereum comunque non è l'unica piattaforma Dapps. Infatti, Ant-share, meglio conosciuta come "Neo" a seguito della ribrendizzazione del precedente marchio di poco successo, punta ad essere la piattaforma Dapps per eccellenza annoverando molte Dapps importanti e di successo tra cui Adex, uno dei

[6] Rete di computer nel quale ogni computer funge sia da client che da server, tengo ad evidenziare che ogni computer può assumere entrambi gli stati, quando mette a disposizione dei propri file sarà il server e gl'altri computer che lo vogliono scaricare/ricevere sono definiti client per quel file , perché a loro volta possono essere server per altri file messi a disposizione della rete. Questo sistema ha permesso di velocizzare molto il download di file perché si evita che tutti i computer siano connessi per tutti i file ad un solo server, oggi tali sistemi sono usati principalmente per trasferire file audio e video o progetti di ogni genere.

pochi exchange decentralizzati, e Red pulse, giornale indipendente con lo scopo di condividere news di tipo finanziario riguardanti in particolar modo il mercato Cinese.

Secondo David A. Johnston, CEO di "Dapps Venture Fund" [7], esistono tre principali tipi di Dapps che sono:

I. Tipo: applicazioni decentralizzate con una propria blockchain. Quella per antonomasia è il Bitcoin, ma la maggior parte delle altcoin[8] rientra in tale categoria.
II. Tipo: applicazioni che si basano sui protocolli di applicazioni di Tipo I che creano, a loro volta, un protocollo e dei token personali. Omni è la più famosa, delle poche esistenti basata sulla blockchain di Bitcoin, mentre su Ethereum ne troviamo ben di più, tra cui la più famosa è sicuramente Eos[9], una cryptovaluta che mira a creare un sistema operativo integrato in blockchain.
III. Tipo: applicazioni che utilizzano il protocollo di una Dapp di Tipo II, con un proprio protocollo e token. Su Omni, troviamo, ad esempio, Safe che punta alla realizzazione di un sistema di criptazione dei file contenuti nei vari cloud. Mentre su Tron si basano molte Dapps, tra cui la più nota è Odissey. Quest'ultima, in particolare, è una piattaforma, oltre che una cryptovaluta, molto interessante in quanto aspira a migliorare e implementare la sharing economy[10], si basa infatti su una rete P2P in modo da eliminare la presenza di intermediari evitando costi superflui per permettere una crescita del Roi sui singoli prodotti o servizi offerti.

Le poche piattaforme per Dapps create (Dapps di Tipo I) tra cui le due principali Ethereum e Neo, non sono altro che il sistema utilizzato per creare gli Smart Contracts, contratti attraverso i quali si può accedere e interfacciarsi con il database decentralizzato che conterrà i nostri dati riguardanti la Dapp che vogliamo utilizzare.

L'idea degli Smart Contracts, meglio noti come contratti intelligenti, non è affatto recente. Infatti il primo a parlarne fu Nick Szabo, che secondo quanto riporta un articolo del Nasdaq (26 Aprile 2016), li teorizzo già nel 1996 in un articolo da lui pubblicato su Extropy. Erano gli albori della diffusione dei Personal Computer, ma egli sostenne già la possibilità di creare un algoritmo capace di far risparmiare tempo e denaro grazie a contratti standard che potevano

[7] https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md
[8] per altcoin in gergo si intende tutte le cryptovalute diverse dal Bitcoin
[9] Nell'epoca in cui scrivo sta diventando una cryptovaluta indipendente creando la propria blockchain e convertendo i propri token e Tron(TRX) cryptovaluta multivalente che punta a creare un web broadcast aspirando a diventare lo "YouTube" decentralizzato oltre ad essere una cryptovaluta attiva nella ricerca per la risoluzione dei problemi relativi alla scalabilità, ed essere una piattaforma Dapps .
[10] Mi riferisco ai nuovi servizi che hanno avuto grande popolarità tra cui, per citarne alcuni, Uber, Airbnb, DogVacay, Zopa…

essere sottoscritti nella medesima forma da molti utenti e basati su condizioni legate ad eventi conoscibili dalla macchina stessa. Con questo non si vuole eliminare le figure professionali che ogni giorno coadiuvano i soggetti per la formazione di contratti complessi e articolati, bensì utilizzare avvocati ed esperti per la redazione iniziale di contratti semplici e ripetibili in modo da creare contratti standard. Un tipico esempio di applicazione consiste nelle licenze software, che in caso di determinati eventi legati all'uso scorretto da parte dell'utente, o alla scadenza del termine di utilizzo, bloccano la fruizione del servizio. Con il tempo tali contratti si sono evoluti, diventando sempre più complessi, ma è grazie all'ideazione di Ethereum e della blockchain, che inizialmente li ha sfruttati per il funzionamento delle Dapps, che si stanno aprendo nuovi scenari cercando di sfruttare gli Smart contracts basati su blockchain per svariati usi. In particolare in campo economico, grazie all'uso di tecnologie IOT che permettono di collegare in rete macchinari e oggetti, ma anche grazie all'uso dell'intelligenza artificiale.

Quindi gli Smart Contracts basati su blockchain, come in passato, non sono altro che algoritmi creati con nuovi codici di programmazione ad esempio, per la programmazione di contratti su Ethereum, viene utilizzato Solidity.

A confermare l'importanza di tali strumenti in economia deriva dall'assegnazione del premio Nobel per l'Economia nel 2016 a due studiosi Oliver Hart e Bengt Holmstroem, per il loro studio riguardante proprio l'architettura dei nuovi tipi di contratti programmabili[11].

Rispetto ai precedenti contratti programmabili sono state introdotte delle novità abissali, in quanto i cosiddetti Smart Contracts consentono:

1) La memorizzazione cronologica di tutti i contratti stipulati da un determinato soggetto e il suo comportamento, permettendo un controllo immediato da parte di autorità esterne o di nuovi contraenti senza perdita di tempo o di informazioni.

2) L'indipendenza: rendendo possibile la creazione, entro certi limiti, di contratti senza la necessità di rivolgersi ad alcun intermediario (un avvocato o un esperto in un determinato settore). Questo permetterebbe un risparmio di tempo e denaro ma, allo stesso tempo, si preverrebbero errori dovuti dalla compilazione manuale dei singoli atti.

3) La fiducia e la sicurezza: questa è la garanzia più importante che possono fornire, in quanto il contratto verrà criptato e duplicato nei vari server decentralizzati ma,

[11] Articolo del 16 Ottobre 2016 del " Il Sole 24 Ore"

soprattutto, verrebbe eseguito solo al verificarsi della condizione contenuta in esso e in modo automatico. In questo modo si ha un contratto incorruttibile ed auto eseguibile.

Ovviamente, come per gli algoritmi precedenti, ci sono alcuni problemi che non sono stati risolti perché di fatto imprevedibili: si tratta di tutti gli inconvenienti che possono derivare da cause esterne, quali eventi climatici, o impedimenti alla connessione alla rete o altri eventi di forza maggiore.

Per spiegare meglio il loro funzionamento e rendere meno vago il concetto, è necessario capire come questi contratti possono essere utilizzati.

Prendiamo allora in considerazione proprio le loro funzioni base, che consistono nella capacità di fornire una serie cronologica dei contratti stipulati da un soggetto e la capacità di tali contratti di detenere denaro sotto forma di cryptovaluta.

Ad esempio, possono essere utilizzati in ambito giuridico, per evitare eventuali contenziosi e lungaggini giudiziarie in caso di spartizione ereditaria. Infatti il de cuius prima della propria morte potrebbe stipulare uno Smart Contract riguardante tutte le proprietà possedute garantendo la possibilità di effettuare un controllo immediato da parte della Blockchain stessa sull'effettiva proprietà o meno di tali beni in quanto risulterebbe possibile la ricostruzione storica dei contratti stipulati in modo immediato all'esecuzione dell'algoritmo. Potrebbe inoltre depositare nel medesimo Smart Contract, Ethereum pari al valore della propria liquidità.

I beni verranno spartiti nel caso del suo decesso alle persone espressamente indicate, mentre gli Ethereum verranno distribuiti tramite i wallet address inseriti. Inoltre, il momento della spartizione/esecuzione sarebbe nota dallo Smart Contract stesso attraverso l'accesso a banche dati Comunali o dell'Inps e il contratto verrebbe immediatamente eseguito.

Si tratta di un semplice possibile utilizzo dei cosiddetti "Smart legal Contracts" in ambito legale ma, ovviamente, possono crearsene di più complessi con il tempo, dato che ci troviamo in un campo nuovo tutto da esplorare. In questo particolare settore degli Smart Contracts di tipo legale è attiva la più grande community internazionale, denominata Legal Hackers che svolge seminari per "avvocati 4.0", ovvero per coloro che si affacciano all'uso dei primi Smart Contracts nel loro lavoro.

Gli Smart Contracts, inoltre, hanno reso possibile la creazione di quelle che vengono definite Smart Property (proprietà intelligenti). Per comprendere il loro funzionamento, bisogna prima comprendere un ulteriore uso che si può fare degli Smart Contracts: attraverso di essi è possibile creare un'identità digitale contenente tutte le proprie informazioni in modo da poterla utilizzare nella fruizione di vari servizi. Infatti sarebbe nota immediatamente tramite l'id del contraente all'instaurarsi di una contrattazione, in modo da permettere di conoscere la controparte sulla

base delle informazioni registrate. Sarebbe una cosa importante se i Governi permettessero la creazione di tale identità a tutti, ma, per ora, vi sono varie rigidità nell'uso di tale tecnologie.
Questo a ben vedere non rappresenta un problema: chiunque attraverso uno Smart Contract può crearsela autonomamente! Ciò gli consentirebbe di sfruttare tecnologie IOT, che a loro volta consentono l'interazione con apparecchiature domotiche, che si potrebbero accendere o rendere funzionali solamente allo Smart contracts indicato dal possessore, le Smart Property.
Proprio in questo settore sta lavorando una newco tedesca: Slock.it[12] , che sta implementando un'applicazione di contratti intelligenti basati su Ethereum, in modo da consentire il noleggio di case, libri, bici e veicoli. Ciò risulterebbe possibile in quanto il proprietario di un bene potrebbe affittarlo o noleggiarlo rendendolo fruibile solo a coloro che acquistino lo Smart Contract che riguarda il bene per un determinato periodo di tempo stabilito in modo automatico tramite applicazione: in questo modo il pagamento e la fruizione saranno immediati, senza bisogno della presenza dell'affittuario.
La funzione di concedere in affitto un bene risulta già possibile grazie alla sua piattaforma, ma è in fase di miglioramento utilizzando la proprietà degli Smart contracts sopra citata in modo da poter controllare l'identità del soggetto fruitore del bene, in questo modo il proprietario potrebbe conoscere il suo contraente sulla base di medesimi contratti precedenti e decidere o meno se concedere il bene in locazione, con pagamento anticipato al momento dell'uso evitando il rischio di credito.
Slock.it non ha intenzione di fermarsi a tale basilare funzione, che già pure taglierebbe fuori dal mercato Airbnb, permettendo la realizzazione di una vera Sharing Economy eliminando ogni intermediario e permettendo una contrattazione C2C diretta. In base al loro progetto, infatti, risulta che abbiano intenzione di permettere addirittura la vendita delle proprietà, cosa che non appare difficile in quanto è sufficiente consentire il trasferimento di tutti gli Smart Contracts che controllano la proprietà al nuovo proprietario e, grazie all'utilizzo della Blockchain risulterebbe possibile mantenere in modo cronologico tutti i trasferimenti di ogni proprietà e, in questo modo nel caso in cui il soggetto cedente non fosse il vero proprietario, il contratto non verrà eseguito in quanto prima della sua esecuzione verrà effettuato tale controllo.
Ovviamente non appare poi così semplice tale integrazione. Il trasferimento della proprietà è effettuabile ma non risulterebbe legalmente valido poiché lo Smart Contract, dovrebbe essere in grado di registrare il trasferimento della proprietà in registri immobiliari e catastali (al momento non possibile) e comunque ogni Stato ha proprie leggi sul trasferimento di proprietà, rendendo così difficile una integrazione su scala globale.

[12] https://slock.it/

Anche in Italia ci sono i primi esempi di applicazione dei contratti intelligenti in economia.
In particolare vorrei segnalare Spindox, una società operante nel settore software che fornisce applicativi di ogni genere alle imprese in modo diligente garantendo un supporto e manutenzioni costanti. Nei primi mesi del 2018 ha iniziato un progetto molto interessante[13] che consiste nel combinare la Blockchain con la logistica, in modo da ottenere una tracciabilità di tutti i passaggi che intervengono lungo la filiera produttiva. Questa ideazione permetterebbe di verificare automaticamente le parti coinvolte nello scambio, in modo che siano affidabili e sicure. In pratica una volta che un soggetto acquista un determinato quantitativo di merce, verrebbe stipulato un contratto intelligente contenente gli estremi delle parti che l'hanno stipulato e la data di effettiva consegna, si genererà poi automaticamente un codice che permette di verificare la corretta esecuzione del trasferimento. Alla consegna, infatti, il codice di verifica deve coincidere con gli ordini di quel determinato giorno, altrimenti o è errato il carico o il giorno di consegna. Questo sistema permette così una migliore tracciabilità del prodotto in fase di spedizione potendo risolvere problemi soprattutto nel traffico internazionale di merci, agevolando enormemente i controlli lungo la filiera produttiva e, a sua volta si andrebbero anche a ridurre i rischi di frode e insolvenze, semplificando la spedizione tramite un alleggerimento del processo documentale che affianca il prodotto. La Dapp web da loro ideata si baserebbe su tre principali pilastri ovvero:

1) L'utilizzo di Ethereum come piattaforma per la creazione di Smart contracts e per la semplicità dei linguaggi di programmazione di derivazione Python, Go e Lisp.

2) L'utilizzo di Swarm come piattaforma cloud decentralizzata, in quanto in un cloud di tipo centralizzato i contratti Smart sarebbero salvabili come algoritmi ma non verrebbero automaticamente eseguiti.

3) L'utilizzo di Whisper come protocollo di messaggistica decentralizzato, in quanto consente un contatto diretto con i fornitori ed eventuali clienti.

[13] https://www.spindox.it/it/blog/blockchain-logistica-smart-contract

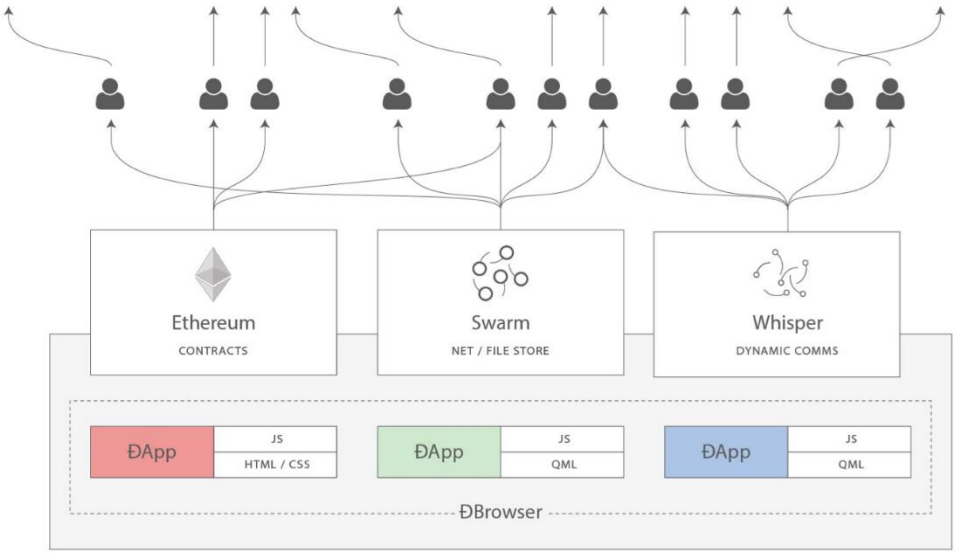


Figura 4: Pilastri della Dapp creata da Spindox

Fonte: https://www.spindox.it/it/blog/blockchain-logistica-smart-contract

Un ultimo importante esempio di utilizzo degli Smart Contracts è nel campo degli attuali (e futuri) fenomeni migratori. In particolare, il World Food Programme dal 2016 ha attivato il progetto "Building Blocks"[14], per il momento in via sperimentale a Zaatari[15] in Giordania, con lo scopo di facilitare gli aiuti internazionali.

Il progetto consiste infatti nel permettere ai rifugiati ospitati nel campo di ottenere un portafoglio digitale su tecnologia Blockchain che, consentirebbe loro di accreditare in tempo reale i sussidi ricevuti, eliminando così tutti gli intermediari lungo la "Catena umanitaria". È stato stimato che questa nuova procedura potrebbe comportare un risparmio del 98% dei costi, in quanto verrebbero eliminati i costi per l'intermediazione bancaria ed eventuali costi di intermediari che lucrano lungo la filiera distributiva. Più nel dettaglio, si sta sviluppando un metodo di pagamento innovativo, denominato "e-pay", che consiste nel pagamento e riconoscimento tramite la retina oculare. Grazie alla blockchain ciò è possibile sfruttando le proprietà di Ethereum e degli Smart Contracts: all'ingresso nel campo, ciascun rifugiato sarà registrato nel sistema governativo attraverso la creazione di uno Smart contracts contenente la propria identità digitale collegata alla propria retina e verrà creato anche un conto digitale, collegato, utilizzabile per pagare tramite una scansione della retina in modo rapido e, ovviamente, sicuro, i beni di cui necessita all'interno del campo. Tale tecnologia non rimane fine a sé stessa per la sola vita all'interno del campo: il portafoglio digitale è utilizzabile anche al di fuori, tramite uno smartphone presso vari negozi o per accreditare l'eventuale stipendio di

[14] https://innovation.wfp.org/project/building-blocks
[15] uno dei campi profughi più grande al mondo avendo una disponibilità per contenere circa 79000 persone

un'attività lavorativa, oltre che avere sempre a portata di mano il passaporto e documenti di riconoscimento. A questo progetto stanno cooperando molti enti tra cui anche Microsoft e Accenture, in modo da riuscire a sviluppare il sistema delle identità digitali, sostenendo il Building Blocks con il progetto ID2020 per garantire a tutti, un'identità digitale e decentralizzata per sgominare il mercato delle contraffazioni e dei traffici illeciti di migranti.

2.2 Ico, Ipo e Start-Up

La piattaforma Ethereum ha una notevole importanza nel mondo delle cryptovalute in quanto permette la formazione di numerosissime ICO (Initial Coin Offer).
Le ICO consistono nella vendita di token (nuova cryptovaluta), al fine di finanziare una società emittente, che potranno poi essere usati dagli acquirenti per pagare il servizio che verrà offerto una volta che la società sarà effettivamente operativa (una sorta di pay in kind). L'acquisizione dei token di una nuova società avviene mediante cryptovaluta, solitamente in Ethereum dato che le Ico spesso sono basate sulla propria piattaforma, ma in rari casi l'acquisto è anche possibile mediante Bitcoin o addirittura in USD.
Questo sistema d'avanguardia permette alla società di nuova formazione di avere in anticipo i fondi raccolti, garantendo allo stesso tempo una partecipazione molto più ampia rispetto ad una IPO (Initial Pubblic Offer) sia perché viene sfruttato il network, sia perché spesso il minimo ammontare per partecipare ad una Coin Offer si aggira intorno a 0.1 eth (al cambio attuale circa 40$). Questo fattore aumenta la partecipazione, tanto che se l'idea risulta fattibile e innovativa, si riescono a raccogliere anche ingenti quantitativi di capitale, in breve tempo.
Da quanto sopra, seppur brevemente esposto, si possono individuare già significative differenze tra ICO e IPO:

1) la prima avviene mediante l'acquisto di token, che possono essere considerati una sorta di ibrido tra un'azione[16] (dato che il token può addirittura essere quotato Exchange) e una moneta di scambio per l'acquisto di un prodotto futuro (dato che non si acquisisce il diritto di essere soci, bensì il diritto di ottenere in futuro un certo servizio o prodotto); mentre la seconda avviene tramite azioni.

[16] Alcune distribuiscono pure dividendi: ad esempio Neo distribuisce Gas, una cryptovaluta quotata utilizzata per pagare le fees delle transazioni in Neo.

2) L'ICO è molto più rapida a realizzarsi, durando alcuni giorni o al massimo uno o due mesi, permettendo inoltre l'accesso anche a piccoli investitori diversamente una IPO, può essere ristretta solo ad investitori istituzionali e richiede diversi mesi per giungere a termine.

Le Ico, inoltre, presentano un ultimo ulteriore vantaggio: data l'assenza in molti Paesi di una regolamentazione adeguata dei mercati finanziari, l'operazione è esente da tassazione.
Questo vuoto legislativo, al contempo, si trasforma nel più grande svantaggio: la difficoltà di riconoscere i progetti reali da progetti falsi o "schemi Ponzi". Negl'ultimi mesi invero la situazione sta cambiando, soprattutto negli USA, dove la SEC sta eseguendo maggiori controlli a seguito del considerevole ammontare di capitale raccolto in ICO, che ha superato i 2 miliardi di dollari (Sole 24 Ore, Ottobre 2018). A riguardo si ricorda il caso del funding di Slock.it (già citata in precedenza), nel quale la SEC, con comunicazione n. 81207 del 25 luglio 2017, affermava che i token venduti rappresentavano securities e in quanto tali si è tenuti a rispettare le leggi federali in materia. Con una comunicazione successiva del 25 Settembre 2017, la SEC ha poi annunciato l'istituzione di una "Cyber Unit", che avrà lo scopo di evitare eventuali condotte illecite assunte dagli operatori sia sulle ICO che in transazioni virtuali su piattaforme di trading.
Per quanto riguarda gli altri paesi, tra cui soprattutto l'Europa e in parte l'Asia (Cina esclusa in cui il Governo è molto attivo intervenendo e vietando le Ico ritenute sospette), si è ancora distanti da ogni regolamentazione, in Italia la Consob non ha mai preso alcuna posizione.
Le IPO, al contrario, come noto sono ampiamente regolamentate e per questo, l'accesso al mercato di capitali è limitato alle società che ne rispettano i requisiti.
Quindi secondo quanto detto sin qui, l'istituzione di una ICO sembra il miglior modo per finanziare la creazione di una nuova società per poter raccogliere fondi in modo efficace e in un lasso di tempo molto breve, tanto che potrebbe risolvere uno dei principali problemi che affliggono le Start-Up[17].

[17] Come ho potuto anche verificare durante il mio stage in Riskapp (Start-Up operante nel settore insurtech che punta, tramite il proprio software, a facilitare all'agente assicurativo la stima di aziende medio piccole tramite vari tool in modo da evitargli un sopraluogo per stipulare una polizza), ovvero la difficoltà nel reperire fondi, tanto che di frequente sono costrette a rivolgersi ad acceleratori, i quali ne approfittano chiedendo quote di capitale e offrendo fondi da poter sfruttare molto spesso solo per acquisire servizi offerti dallo stesso, quindi sostanzialmente un finto finanziamento, che in casi limitati porta al successo della Start-Up.

2.3 Ripple e il superamento delle camere di compensazione

Ripple è una valuta digitale anch'essa, basata su blockchain ma si caratterizza per la presenza di registri delle transazioni, chiamati ledger, che permettono di monitorare gli scambi e consentono di ottenere una velocità maggiore nel trasferimento di denaro (l'esecuzione impiega pochi secondi). Inoltre, è l'unica cryptovaluta ad essere centralizzata in quanto emessa e gestita dai Ripple Labs di San Francisco, mentre le altre cryptovalute sono gestite da una community di sviluppatori e spesso quindi sono open source. Possiamo quindi definire Ripple una sorta di ibrido: è pur sempre una cryptovaluta, con tutti i benefici che ciò comporta (assenza intermediazione, basse fees per le transazioni e privacy delle stesse), ma, allo stesso tempo, è centralizzata. Quest'ultima qualità, che la rende di fatto controllabile, gli ha consentito di ottenere partnership e risorse finanziarie dalle principali banche (tra cui Unicredit, Credit Agricole e Santander) che la possono utilizzare per i pagamenti dei propri clienti su scala internazionale, ma, anche da fondi d'investimento e società per il trasferimento di denaro, tra cui Moneygram, che ha avuto anche modo di testarla per alcuni pagamenti internazionali. Ripple, infatti, si basa su un protocollo peer to peer ma, in questo caso, le nuove cryptovalute non vengono "minate, estratte" (come tutte, o quasi, le altcoin), bensì si possono solo acquistare nel mercato[18]. Ecco perché ritengo che sia una cryptovaluta centralizzata: proprio perché, la Ripple Labs può decidere quante farne circolare (quantità offerta) facendo variare quindi il prezzo.

Ripple(XRP) quindi oltre che essere controllabile (caratteristica gradita dagli enti finanziari), possiede basse fees per ogni transazione, infatti vengono trattenuti e distrutti 20 drops (unità minima di XRP) che corrispondono a 0,0002(XRP)=0.0001€ al cambio attuale, dal proprio conto. Un'altra cosa da sapere, non molto nota, è che per utilizzare un wallet Ripple devono essere depositati almeno 20 (XRP) per evitare la creazione di conti spam, bot o inutilizzati dagli utenti.

A questo punto mi preme fare una precisazione.

Ripple(XRP) come cryptovaluta, può essere utilizzata, come le altre cryptovalute, per scambiare valore tra più soggetti, anche per scambi transazionali.

È questa infatti l'utilità che intravvedono le banche commerciali o i money transfer operators partner del progetto.

[18] Anche se è da sottolineare che, inizialmente, vennero elargite anche a coloro che avevano contribuito alla sua creazione, o alla creazione di sue parti di codice, durante veri e propri concorsi per esperti di programmazione, in modo da migliorare la qualità del proprio servizio.

Eppure, la mission e vision della società Ripple Labs, è tutt'altra cosa, XRP non ambisce ad essere (l'ennesima) nuova valuta, ma vuole servire, al sol fine di pagare le fees, o meglio, il servizio che viene svolto, che coincide con il trasferimento di valuta fiat da un soggetto ad un altro!

Si tratta quindi di un uso marginale della cryptovaluta, che però rimane interessante comprendere più a fondo.

La Ripple Labs ha creato tre protocolli (Xrapid, Xvia e Xcurrent) per effettuare trasferimenti internazionali in modo da evitare le stanze di compensazione e eventuali intermediari lungo la filiera del pagamento. Le stanze di compensazione, che in Italia sono istituite presso la Banca d'Italia, non sono altro che un sistema utilizzato per la regolazione dei conti tra le varie banche aderenti. Nello specifico, le clearing house amministrano dei registri per ciascuna banca e in ciascuno di essi sono segnati i crediti verso le altre banche (es: Deposito di un assegno tratto su altra banca, deposito su sportelli di altre banche…) o gli eventuali debiti, in modo da poter calcolare giornalmente il proprio credito/debito netto nei confronti di ciascuna banca aderente. Le stanze di compensazione, di fatto, semplificano enormemente il lavoro delle singole banche in quanto permettono di evitare l'effettuazione di operazioni superflue, compensando il regolamento tra le banche stesse.

Le banche, d'altra parte, devono passare per le stanze di compensazione per tutti, o quasi, i pagamenti internazionali che intervengono tra due soggetti, l'invenzione di Ripple permette la rimozione delle stanze di compensazione, evitando inoltre l'aggiornamento di svariati registri e l'eliminazione dei costi per le transazioni interbancarie.

Permette anche, di eliminare gli eventuali intermediari di cambio, in quanto il cambio verrà effettuato tramite i cosiddetti liquidity provider, ovvero organizzazioni finanziarie che offrono la loro proposta di cambio, e nell'esecuzione verrà scelto il miglior tasso sul mercato al momento della transazione in maniera automatica.

Questo permette (vedi immagine sottostante) un collegamento diretto tra due banche, in qualsiasi parte del mondo in cui si trovino bypassando le clearing house.

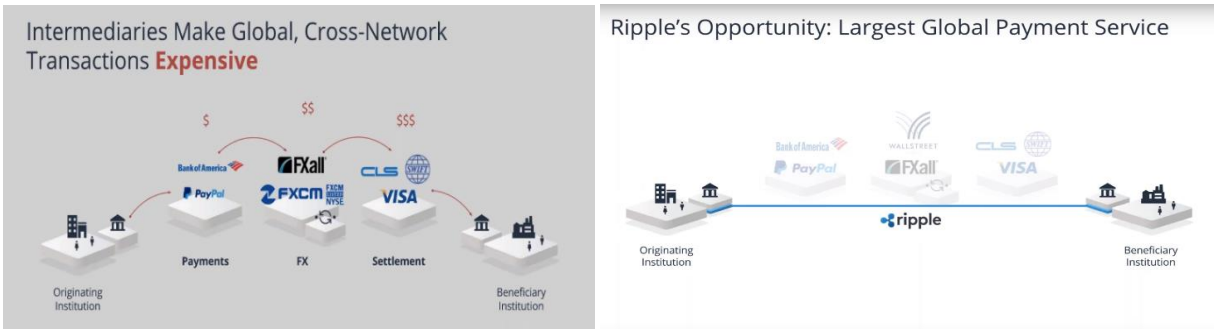


Figura 5: Trasferimenti di denaro senza e con l'uso di Ripple

Fonte: **https://ripple.com/collateral/**

Il trasferimento bancario tramite la piattaforma Ripple, secondo quanto enunciato nel sito della società[19], avviene tramite i tre protocolli: Xcurrent, Xvia e Xrapid, i quali permettono di ottenere un vantaggio consistente nel tempo in cui viene eseguita la transazione che risulta nell'ordine di 3 a 8 secondi, rispetto ai 2/3 giorni lavorativi di un normale bonifico effettuato tramite protocollo Swift.

L'Xcurrent viene utilizzato per pagamenti di medesima valuta, che non necessitano quindi di un cambio, e funziona in modo semplice, lineare e trasparente. Esso opera su due livelli: un primo livello consiste in un tool per la messaggistica, che consente alle banche di inviarsi messaggi tra loro in modo da coordinarsi per effettuare la transazione; un secondo livello è costituito da un registro, che consente l'effettuazione della transazione in modo automatico, veloce e trasparente di cui già parlavo sopra ovvero l'ILP Ledger che coordina il trasferimento del denaro tra le due istituzioni bancarie. Il protocollo permette, inoltre, la conversione dei messaggi delle banche in formato Swift FIN o Iso, che è il formato standard per i messaggi di tipo finanziario.

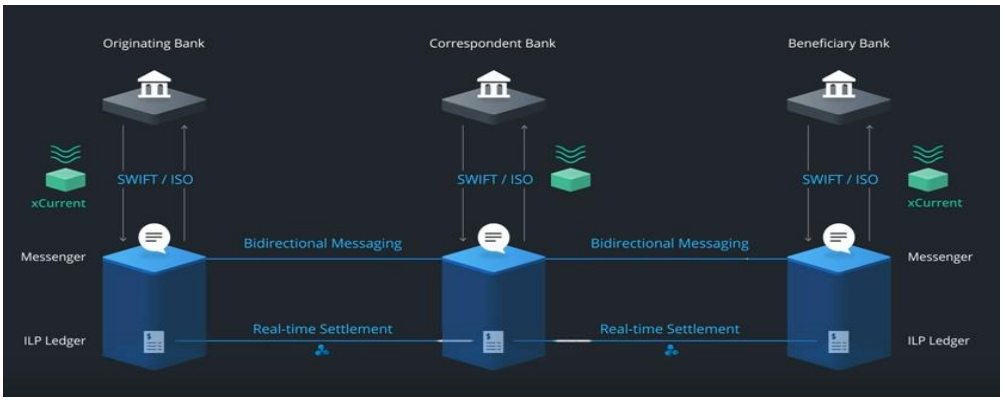


Figura 6: Trasferimento con il protocollo Xcurrent

Fonte: **https://ripple.com/solutions/process-payments/**

[19] https://ripple.com/

Possiamo quindi ripercorrere come avviene effettivamente il pagamento, che coinvolge tre intermediari: la banca mandataria, una banca di corrispondenza e la banca beneficiaria.
Viene dapprima spedito un messaggio alla richiesta dell'operazione, tramite il primo livello del protocollo alla banca corrispondente e alla banca beneficiaria; il protocollo, consente in automatico una verifica sul database della banca beneficiaria della correttezza dei dati inseriti rispetto al numero di conto e al soggetto detentore, mentre il messaggio inviato alla banca corrispondente serve per calcolare le fees per la transazione, ottenendo quindi il costo totale della stessa. L'intero processo di verifica impiega qualche secondo ed opera in background.
Nel caso in cui le informazioni inserite non dovessero essere corrette, la transazione non sarà effettuata, mentre se lo sono, si passa all'utilizzo del secondo livello del protocollo.
Viene ora criptata la transazione e viene in contemporanea eseguita la verifica del reale possesso di fondi del mittente per sostenere i costi della transazione; a verifica ultimata il pagamento verrà eseguito in pochi secondi in maniera più economica e con la possibilità di verificare tutte le operazioni che sono intercorse durante la transazione rendendole più trasparenti anche per eventuali controlli di enti esterni.
L'Xrapid invece è un altro protocollo che spesso è integrato nell'Xcurrent, ma non necessariamente. Questa, secondo me, è la novità più importante ed efficace apportata da Ripple: attraverso questo protocollo avviene il cambio di valuta per i pagamenti internazionali attraverso l'Xcurrent. Al momento del pagamento (che necessita di una conversione di valuta) il protocollo rende immediata la conversione al miglior tasso proposto nel mercato, tra una valuta fiat e Ripple(XRP). Tale operazione valutaria avviene molto più velocemente rispetto alle soluzioni attuali sul mercato; una volta a destinazione, il valore in XRP verrà nuovamente convertito al minor tasso di cambio in valuta fiat del richiedente.

Figura 7: Trasferimento con il protocollo Xrapid

Fonte: **https://ripple.com/solutions/source-liquidity/**

Per ultimo, il protocollo Xvia, che si distingue dai precedenti:

1) per la tipologia di target a cui si rivolge, ovvero ad imprese e non ad enti finanziari;

2) per le funzioni implementate, che consentono alle imprese di spedire denaro tra loro utilizzando unicamente la blockchain Ripple, senza che sia necessario scaricare alcun software ma agendo tramite API.

Il protocollo suddetto consente, oltre al tracking, anche l'inserimento di documenti allegati al pagamento (ad esempio, fatture di vendita), semplificandone la loro archiviazione dato che sono allegati ad un pagamento e sempre disponibili per essere confrontati e stampati.

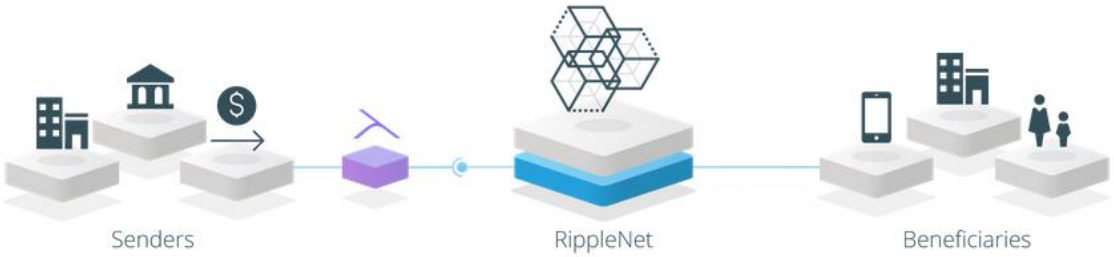


Figura 8: Trasferimento con il protocollo Xvia
Fonte: **https://ripple.com/solutions/send-payments/**

Tutte le soluzioni innovative di Ripple sono in parte già prassi quotidiana.
Banco-Santander, infatti offre ai suoi clienti un nuovo servizio basato sulla blockchain Ripple denominato "One Pay FX" per permettere pagamenti internazionali istantanei utilizzando contemporaneamente sia il protocollo Xcurrent che Xrapid (CNBC, Aprile 2018).[20] Oltre agli enti bancari, che stanno sperimentando Ripple, si annoverano anche due dei più grandi money transfer del mondo: la Western Union (CNBC Febbraio 2018) e Moneygram (CNBC Gennaio 2018), quest'ultimo già finanziatore e partner del progetto, tanto che potrebbe sfruttare la situazione a suo vantaggio per battere il rivale storico.

[20] Questo servizio è attualmente operativo nelle filiali in Spagna, Regno Unito, Polonia e Brasile.

CAPITOLO 3: Rivoluzione o Innovazione?

LE CRYPTOVALUTE SONO, A SECONDA DI COME LE SI GUARDA, SIA UNA RIVOLUZIONE CHE UN'INNOVAZIONE: SONO UNA RIVOLUZIONE IN QUANTO STANNO CAMBIANDO IL NOSTRO MODO DI RAPPORTARCI ALL'ECONOMIA, MENTRE UN'INNOVAZIONE SE CONSIDERATE SUL PIANO TECNOLOGICO.

3.1 Analogie e differenze con Internet a livello tecnologico

A mio modo di vedere, vi sono molte analogie tra l'invenzione delle cryptovalute e quella di internet o delle società Dot-com che hanno aperto la strada per una quarta rivoluzione industriale, Internet 4.0, dove autoveicoli, macchinari ed elettrodomestici sono collegati nella rete web.

La nascita delle cryptovalute, oltre che essere l'espressione di una voglia di cambiamento del modello economico dominante[21], slacciandosi da organismi istitutivi e di controllo, che molto spesso hanno agito in modo non trasparente, è da considerarsi come un progresso in campo tecnologico dato che si basa su una tecnologia pregressa: Internet.

Molto probabilmente senza la precedente invenzione di Internet, le cryptovalute non sarebbero mai nate, in quanto non ci sarebbe l'odierna infrastruttura di rete da cui, poterne creare una addirittura decentralizzata e complessa, quale è la Blockchain. Ricordo infatti che erano già nati applicativi per connettersi sfruttando internet in modo "peer to peer" come ad esempio i programmi di Torrent, che permettevano di condividere file (film e musica principalmente) in modo più veloce tra pc in rete senza passare attraverso un server (che rallentava l'invio di pacchetti quando molti pc contemporaneamente scaricavano da esso).

La differenza principale tra le due invenzioni è proprio la decentralizzazione, ovvero un collegamento differente tra i diversi computer. Ciò infatti avviene sempre nell'ambito di una "rete di reti", ma in questo caso non vi è un collegamento client-server di tipo gerarchizzato, ma un collegamento biunivoco tra un client, che può diventare server, e un server, che a sua volta può diventare client: tutto dipende dal ruolo dei singoli nodi nello scambio di dati, file o moneta; come nel caso in parola.

[21] Ed in quanto come ogni altra invenzione "dirompente" è ostacolata da chi la percepisce come minaccia allo status quo

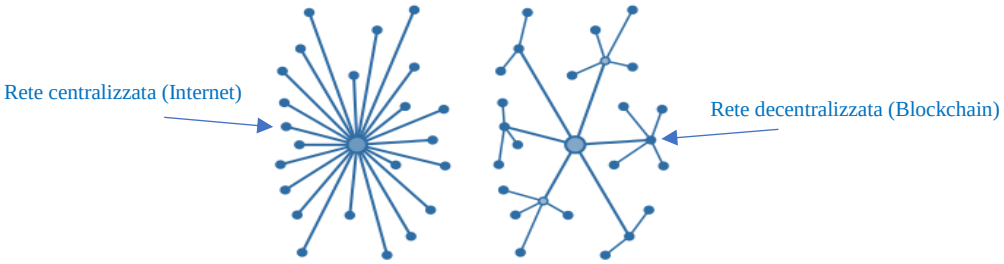


Figura 9: Topologie di rete

La topologia di rete decentralizzata Blockchain (fig.9) offre una sicurezza maggiore, dato che ogni nodo può fruire da server in caso di necessità, in quanto le copie dei registri sono salvate in modo identico in ciascuno di essi.

Le cryptovalute però hanno introdotto, a seguito della creazione di Iota, una rete distribuita oltre che decentralizzata portando ad una vera e propria innovazione con il protocollo Tangle, il quale permette una scalabilità e velocità maggiore per le transazioni.

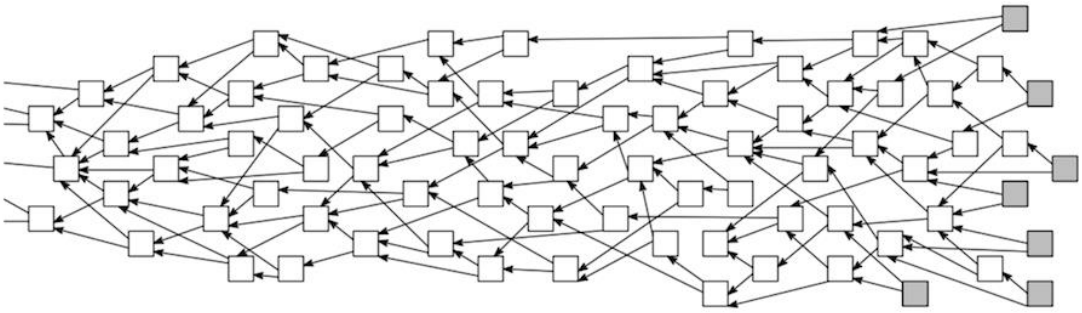
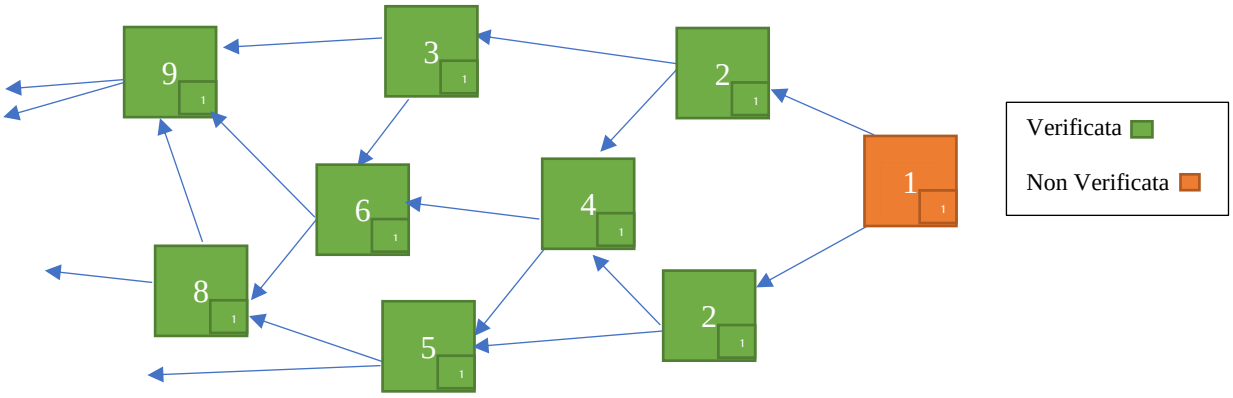


Figura 10: Protocollo Tangle

Fonte: https://www.nasdaq.com/article/what-is-the-tangle-and-is-it-blockchains-next-evolutionary-step-cm911074

Tale protocollo funziona in un modo totalmente differente dalla Blockchain in quanto, prima di tutto, non esiste alcun miner per le transazioni; quindi non si devono sostenere fees per effettuarle e al contempo la scalabilità è maggiore, ovvero possono eseguirsi più transazioni al minuto rispetto al Bitcoin e le altre cryptovalute (risparmiando anche molta potenza elettrica). Il suo funzionamento è anche molto semplice (fig.10): ogni quadrato di questa topologia di rete, definito "Site", indica una transazione e contiene tutte le informazioni riguardanti il mittente, il ricevente e l'ammontare di cryptovaluta inviato. I vari Site sono collegati a due a due tra di loro formando delle connessioni, chiamate in gergo "Edges", che sono il fulcro di tale sistema: grazie ad esse si possono verificare le transazioni effettuate in rete precedentemente. I nuovi nodi che inviano cryptovaluta sono infatti tenuti a verificare i due precedenti Site a cui si collegano. Ogni verifica che viene effettuata è una confirmation; maggiore è il loro numero,

maggiore è la sicurezza che una transazione sia stata effettuata correttamente: molti wallet ne richiedono più di venti per effettuare la transazione e vedere accreditato l'importo ricevuto.
Quindi ogni singolo Site ha un numero di confirmation, che si configura come cumulative weight che altro non è che la $\sum weight\ dei\ Site\ precedenti\ collegati$ sia direttamente che indirettamente. Ogni Site ha un valore pari a 1 e ogni volta che si collega un nuovo Site il cumulative Weight di ogni singolo Site aumenta come rappresentato nell'esempio sottostante.



Ecco come questo sistema distribuito permette di risolvere anche alcuni problemi che a lungo andare potrebbero inficiare il sistema Blockchain.
Infatti la Blockchain, per effettuare una transazione in uscita dal proprio wallet offline [22] o vedersi accreditato l'importo ricevuto, richiede che la cronologia delle transazioni sia aggiornata all'ultima transazione effettuata nel mercato, dato che si tratta di un registro decentralizzato e che ogni nodo deve disporre di copie identiche. Attualmente l'intero registro Blockchain risulta pesare più di 50 GB, ma è in continuo aumento: con il trascorrere del tempo renderà difficile, soprattutto per dispositivi obsoleti, memorizzare l'intero registro. Il protocollo Tangle, invece, richiede la sola memorizzazione in locale di una parte delle transazioni a cui allacciarsi, questo consente di utilizzare i wallet offline per la prima volta anche su dispositivi mobili.
Anche Tangle tuttavia ha un problema, che non la rende affidabile: la sicurezza[23].

[22] I wallet online al contrario dispongono sempre della cronologia delle transazioni effttuate agiornata dato che sono sempre collegati in rete, ma di fatto sono gestiti in modo centralizzato ovvero si basano sui server del gestore, che è quasi come una banca, e spesso applica fees più alte nei trasferimenti o cambi non proprio vantaggiosi.
[23] Da quanto traspare, i programmatori della società stanno lavorando ad un miglioramento che potrà realizzarsi con un probabile fork.

3.2 Rivoluzione economica delle cryptovalute

La rivoluzione apportata dalle cryptovalute, a mio sommesso modo di vedere, è avvenuta in campo economico: creando un nuovo paradigma economico per cercare di limitare l'intervento di intermediari, risparmiando così anche i costi di ciascuna transazione. Le cryptovalute sono nate nel 2008 a seguito dell'ennesima crisi borsistica, e alla pessima gestione di essa da parte delle istituzioni, come un'alternativa alle monete aventi corso legale.
Vorrei partire a spiegare la rivoluzione delle cryptovalute da una celebre frase di Douglas North, premio Nobel per l'economia nel 1993 (Economic Performance Through Time, 1994):

"Istitutions are the humanly devised constraints that structure the human interaction. They are made up of formal constraints (e.g., rules, law, constitutions), informal constraints (e.g., norms of behavior, conventions, self-imposed codes of conduct), and their enforcement characteristics. Together they define the incentive structure of societies and specifically economies. "

Infatti l'uomo, sin dall'antichità, ha creato dapprima delle regole informali che venivano stabilite e fatte rispettare secondo la legge del più forte, ma che con il tempo sono diventate formali per regolare gli scambi tra i singoli soggetti. In epoca più recente si sono formate le prime Istituzioni (banche, governi, società...) in grado di controllare le varie transazioni, in modo da ridurre l'incertezza negli scambi.
Poi, con l'avvento di Internet, è cambiato il nostro modo di rapportarci con le istituzioni che, nella maggior parte dei casi, si sono digitalizzate in modo da velocizzare le transazioni e permettendoci un controllo immediato sulle nostre finanze. Questo ha comportato un aumento della clientela utilizzatrice e delle operazioni eseguite, tanto che si è ridotto il controllo su ciascun individuo. Oggi però, per la prima volta, grazie alla Blockchain, siamo in grado di ridurre l'incertezza nelle transazioni, non solo attraverso istituzioni politiche ed economiche, ma anche grazie alla tecnologia, riducendo enormemente il controllo da parte di istituzioni esterne. Grazie ad essa possiamo infatti risolvere tre principali problemi che si presentano ogni qualvolta decidiamo di effettuare una transazione mediante internet:

1) Incertezza sul contraente: è possibile avere a disposizione lo storico delle varie transazioni effettuate da ogni soggetto raggruppabili in base all'identità digitale di che le ha effettuate (creata con uno Smart Contract), stabilendo un suo rating nelle varie attività online.

2) Tracking dei prodotti: consentendo alle società di avere a disposizione un database decentralizzato in modo da seguire l'intera Supply Chain di molti prodotti contemporaneamente.
3) Transazioni negate: per la prima volta è possibile inviare fondi attraverso uno Smart Contract che contiene un ammontare di denaro che verrà rilasciato al venditore solo se il prodotto arriverà a destinazione.

Si è giunti, inoltre, alla creazione di un sistema indipendente simile al gold standard, in quanto le cryptovalute e l'oro non sono emessi da alcun organismo centrale (rectius, eccetto Ripple), e allo stesso tempo sono limitati in ammontare. Risultano però diversi per velocità di transazione e politiche di estrazione: nel caso dell'oro, sono ragionate e controllate per non aumentare l'inflazione del metallo.
Questo nuovo sistema monetario potrebbe rivoluzionare il mondo bancario facendo risparmiare ingenti costi, non solo derivanti dal risparmio energetico rispetto alla coniazione, ma riguardanti l'intero sistema burocratico che governa la circolazione ed emissione monetaria "nel sistema tradizionale". Troviamo infatti una sorta di piramide gerarchica che vede:

1) Al vertice, i legislatori, le autorità centrali di emissione (Banche centrali) e le Autority di controllo.
2) A lato, i mercati finanziari su cui avvengono le transazioni di capitali.
3) In un livello inferiore, le Banche Nazionali che controllano (o quantomeno cercano) le banche commerciali per tutelare i consumatori, spesso con scarsi risultati[24].
4) Infine, le banche commerciali e di investimento che si rivolgono alla propria clientela.

Tali sistemi di pagamento minano alla secolare posizione dominante delle organizzazioni bancarie, tagliandole fuori dalla creazione e gestione delle cryptovalute, anche per la loro stessa difficoltà di adattamento e lentezza digitale rispetto alla rivoluzione in corso. È pur vero che vi sono anche alcuni colossi bancari che si stanno comunque muovendo per creare una propria cryptomoneta (Utility Settlement Coin)[25] o che si stanno appoggiando ad una cryptovaluta esistente che ritengono adeguata e funzionale alla propria attività (i.e. Santander con Ripple). Al contempo addirittura i governi con le proprie cryptovalute potrebbero porre fine al dominio

[24] I crack bancari sono sempre esistiti e sempre esisteranno, fintantochè le banche saranno imprese e non già istituzioni dell'ordinamento democratico.
[25] http://www.ilsole24ore.com/art/finanza-e-mercati/2016-08-25/big-bank-unite-creare-proprio-bitcoin-063907.shtml?

bancario, un recente tentativo è fornito dal governo della Repubblica Bolivariana del Venezuela, il cui presidente Maduro ha disposto la creazione del "Petro", una moneta digitale nel tentativo di risollevare l'economia del proprio paese e contrastare "il sabotaggio economico commissionato dagli USA"[26]. Lo sbarco sul mercato è già avvenuto raccogliendo già più di 735 milioni di dollari. Oltre ad essere una valuta emessa da uno Stato Sovrano è addirittura una cryptovaluta garantita da un sottostante: le riserve di petrolio, di cui il Paese è primo al mondo per riserve accertate[27].

3.3 Analogie e differenze con Internet a livello economico

La transazione alla Blockchain sarà certamente più lenta e complessa rispetto alla diffusione e utilizzo di internet, che è stato praticamente sin da subito sfruttato a seguito della creazione dei primi sistemi operativi user friendly, con browser preinstallato. Per le aziende invece si trattò di un cambiamento drastico. A quell'epoca molte imprese non cogliendo l'importanza della rete internet e la rivoluzione non solo digitale, ma del paradigma di produzione e scambio in corso, magari per la poca importanza che davano alla nuova tecnologia, hanno visto ridursi la propria market dominance a favore dei concorrenti, oppure più spesso sono state espulse dal mercato. D'altra parte internet è stata la fortuna di nuove società, che prima non sarebbero mai potute entrare nel mercato, in quanto non avrebbero avuto alcuna chance di affrontare i player consolidati in molti settori. In questa situazione si trovò ad esempio "Barners & Noble", società leader nella vendita retail di libri in America operante tutt'oggi, ma che con internet ha visto ridursi la propria market dominance in modo drastico, tanto che ha portato poi al crollo della propria capitalizzazione di mercato (le azioni BKS crollarono di oltre un 60%) a causa di un nuovo player all'ora sconosciuto: Amazon. Amazon nacque di fatto grazie ad internet puntando alla vendita mediante e-commerce di libri, film e CD musicali, ma fu solo dopo la crisi della Dot.com che diventò una minaccia per Barners grazie alla vendita di "Kindle", un lettore per epub che distrusse la vendita retail di libri cartacei, riscontrando sin da subito un grande successo, e consentendo poi ad Amazon di crescere diversificando i propri prodotti.

[26] Cfr. Adam Samson, "*Venezuela launches presale of state-backed 'petro' cryptocurrency*", FT, 20 February 2018.
[27] Fonte: Wikipedia, lemma "List of countries by proven oil reserves".

Figura 11: Andamento borsistico delle azioni delle due società: Barners and Noble (sx), Amazon (dx)

Fonte: https://it.finance.yahoo.com/

Oltre all'esempio di Amazon (fig.11), che tramite l'e-commerce ha distrutto molte imprese del settore retail, passando ad una vendita diretta come grossista, evitando l'ausilio di un dettagliante, vi sono molti altri esempi di società che sono riuscite ad emergere tra cui: Spotify, che sta rivoluzionando il settore musicale; YouTube e le Pay-tv, che stanno rivoluzionando il settore cinematografico; le e-mail stesse, che hanno sin da subito iniziato a sostituire le società dei servizi postali. In generale, però, tutti coloro che non si sono innovati entrando nella rete sono stati sorpassati da coloro che hanno colto per primi tale novità e hanno saputo sfruttarla.
La Blockchain di fatto potrebbe portare a medesimi cambiamenti, se non addirittura più drastici e in molti più settori dell'economia, richiedendo al tempo stesso nuove figure professionali come al tempo anche internet, e una riqualificazione del personale esistente.

3.4 Paragone tra la Bolla Dot.com e Blockchain

Le due rivoluzioni, Internet e la Blockchain, sono state qui comparate sia per il loro duplice profilo, tecnologico ed economico, sia per la forte speculazione che ha portato alla loro affermazione. Sono presenti infatti alcune analogie tra i due fenomeni, anche se la bolla Blockchain ha un ordine di grandezza inferiore di 15 volte rispetto ai trilioni di dollari che portarono allo scoppio della Dot.com:

1) Entrambe si sono sviluppate attraverso un'innovativa modalità di raccolta fondi: le società di Internet si sono basato sulle IPO, mentre la Blockchain sulle ICO, ma con il medesimo obiettivo ovvero la penetrazione del mercato a scapito del profitto.

2) Presentano il medesimo meccanismo speculativo: la semplice aggiunta di Dot.com o Blockchain al nome di una società ne fa aumentare di molto il valore borsistico, in quanto crea enormi aspettative di crescita e utili futuri (un esempio è la società Bioptix Inc che rebrendizzata in Riot Blockchain[28] ha visto il valore delle proprie azioni salire di oltre un 17% in pochi giorni).

3) Come nella Bolla della Dot.com, vi sono alcune società che stanno creando ICO e progetti di nuove cryptovalute senza alcun fondamento. Secondo le stime di Tokendata (La Repubblica, 2018)[29], tra oltre 1500 progetti di cryptovalute il 46% è in qualche modo già fallito. Un esempio è lo schema Ponzi dietro a Bitconnect, cryptovaluta che prometteva, in cambio del deposito in piattaforma interessi molto elevati pagati di fatto con i depositi dei nuovi entranti senza creare alcun valore.

Al tempo stesso però vi sono alcune importanti differenze rispetto alla "bolla .com" di fine anni '90: Bitcoin e le cryptovalute non sono azioni societarie, ma mezzi di scambio che possiedono un valore intrinseco. Infatti analizzando le cryptovalute, e in particolare il Bitcoin, si può notare che esso possiede un valore intrinseco, che differisce dal suo prezzo di mercato, che comprende tutti i costi sostenuti dai miners per estrarlo (costi per l'hardware, elettricità, sistemi di raffreddamento…). Questo valore aumenta nel corso del tempo, dato l'aumento della difficoltà di estrazione: a mano a mano che la cryptovaluta viene estratta, richiede sistemi più potenti. Ad oggi il costo di produzione di un Bitcoin è in media di 6500$[30] (compreso il costo dell'hardware); se il suo valore dovesse scendere al di sotto di tale cifra, i produttori che spendono un maggior costo per l'elettricità saranno costretti ad uscire dal mercato.

[28] https://www.bloomberg.com/news/articles/2017-10-04/from-biotech-to-bitcoin-bioptix-shifts-focus-to-blockchain

[29] http://www.repubblica.it/tecnologia/sicurezza/2018/02/26/news/criptovalute_il_46_di_quelle_lanciate_nel_2017_e_gia_fallito-189821972/

[30] https://it.businessinsider.com/estrarre-bitcoin-e-sempre-piu-costoso-un-esperto-spiega-fino-a-quando-sara-redditizio/

Dove è meno costoso				Dove è più costoso	
Venezuela	531 $	India	3.274 $	Germania	14.275 $
Trinidad e Tobago	1.190 $	Canada (Ontario)	3.965 $	Danimarca	14.275 $
Uzbekistan	1.788 $	Russia	4.675 $	Tuvalu	14.493 $
Ucraina	1.852 $	Stati Uniti	4.758 $	Tonga	14.671 $
Kuwait	1.983 $	Norvegia	7.784 $	Isole Marshall	14.751 $
Bielorussia	2.177 $	Francia	7.930 $	Isole Cook	15.861 $
Bangladesh	2.379 $	Regno Unito	8.402 $	Isole Salomone	16.209 $
Kazakistan	2.835 $	Giappone	8.723 $	Bahrein	16.773 $
Arabia Saudita	3.172 $	**Italia**	**10.310 $**	Niue	17.566 $
Cina	3.172 $	Spagna	11.103 $	Corea del Sud	26.170 $

Figura 12: Costo dell'elettricità per l'estrazione di un Bitcoin nel 2018

Fonte: https://it.insider.pro/infographics/2018-02-01/quanto-costa-minare-1-bitcoin-mining-grafico/

Mentre il suo prezzo è influenzato da due principali fattori: le aspettative tecnologiche sulla cryptovaluta e sul relativo progetto di paradigma economico alternativo, e la crescita di utilizzazione (volume di scambio).

A questo si aggiunge la speculazione di mercato che ovviamente ha contribuito a portare il valore della cryptovaluta ad un prezzo che ha sfiorato i 20.000$ a inizio 2018, una sorta di piccola bolla ormai rientrata.

Concludo quindi rivolgendomi a coloro che reputano il valore del Bitcoin privo di alcun fondamento o che sia solamente una bolla speculativa: è mio convincimento invece che il suo valore attuale lascia ben poco margine di profitto ai produttori ubicati nei paesi più industrializzati, mentre un profitto può essere conseguito solo da coloro che sono operativi in regioni a più basso costo energetico (fig. 12, che però non comprende il costo dell'hardware)[31].

Numero di parole totali esclusa la Bibliografia: 13755

[31] L'hardware è un componente di costo necessario per ridurre i tempi di estrazione: per creare un Bitcoin con una sola macchina, è necessario circa un anno e mezzo.

BIBLIOGRAFIA

ANON, 27 Aprile 2018. Cryptovalute, stroncatura da Bankitalia: "Meccanismo tipico delle bolle speculative". Repubblica[online]. Disponibile su: http://www.repubblica.it/economia/2018/04/27/news/criptovalute_stroncatura_da_bankitalia_meccanismo_tipico_delle_bolle_speculative_-194936886/ [Accessed 29 Apr. 2018]

Balestreri Giuliano, 17 Dicembre 2017. Estrarre bitcoin è sempre più costoso: un esperto spiega fino a quando sarà redditizio. Business Insider[online]. Disponibile su: https://it.businessinsider.com/estrarre-bitcoin-e-sempre-piu-costoso-un-esperto-spiega-fino-a-quando-sara-redditizio/ [Accessed 13 Aug. 2018]

Browne Ryan, 12 Aprile 2018. Santander launches a blockchain-based foreign exchange service that uses Ripple's technology. CNBC [online]. Disponibile su: https://www.cnbc.com/2018/04/12/santander-launches-blockchain-based-foreign-exchange-using-ripple-tech.html [Accessed 05 Jul. 2018]

Cheng Evelyn, 1 Dicembre 2017. JPMorgan strategist: Bitcoin futures can 'add legitimacy' to potential 'emerging asset class. CNBC [online]. Disponibile su: https://www.cnbc.com/2017/12/01/jpmorgan-strategist-bitcoin-futures-can-add-legitimacy.html [Accessed 06 May 2018]

Cipolletta Fiorella, 17 Maggio 2017. Blockchain 'The Next Big Thing. Pubblicità Italia, Pag. 83 N.3. Disponibile su: https://www.reply.com/it/notizie/rassegna-stampa/Shared%20Documents/Blockchain_The_Next_Big_Thing.pdf [Accessed 15 Apr. 2018]

Cosimi Simone, 26 Febbraio 2018. Criptovalute, il 46% di quelle lanciate nel 2017 è già fallito. Repubblica[online]. Disponibile su: http://www.repubblica.it/tecnologia/sicurezza/2018/02/26/news/criptovalute_il_46_di_quelle_lanciate_nel_2017_e_gia_fallito-189821972/ [Accessed 12 Aug. 2018]

Dagnino Francesco, 18 Ottobre 2018. Initial Coin Offering (ICO) e offerta al pubblico di prodotti finanziari. Il Sole 24 Ore [online]. Disponibile su : http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2017-10-18/initial-coin-offering-ico-e-offerta-pubblico-prodotti-finanziari-105639.php? [Accessed 08 Jul. 2018]

Floyd David, 2018. What Is The Tangle, And Is It Blockchain's 'Next Evolutionary Step'?. Nasdaq [online]. Disponibile su: https://www.nasdaq.com/article/what-is-the-tangle-and-is-it-blockchains-next-evolutionary-step-cm911074 [Accessed 19 Jul. 2018]

Gord Michael, 26 Aprile 2016. Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality. Nasdaq [online]. Disponibile su: https://www.nasdaq.com/article/smart-contracts-described-by-nick-szabo-20-years-ago-now-becoming-reality-cm611829 [Accessed 21 May 2018]

Henry David, Anna Irrera, 21 Settembre 2017. JPMorgan's Dimon says bitcoin 'is a fraud'. Reuters [online]. Disponibile su: https://www.reuters.com/article/legal-us-usa-banks-conference-jpmorgan/jpmorgans-dimon-says-bitcoin-is-a-fraud-idUSKCN1BN2PN [Accessed 06 May 2018]

J. Fanusie Yaya and Tom Robinson, 2018. Bitcoin laundering: an analysis of illicit flows into digital currency services. Elliptic[online]. Disponibile su: https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf?t=1525001933973 [Accessed 02 May 2018]

Katz Lily, 4 Ottobre 2017. A Biotech Company Changed Its Name to 'Riot Blockchain' and Its Stock Is Surging. Bloomberg [online]. Disponibile su: https://www.bloomberg.com/news/articles/2017-10-04/from-biotech-to-bitcoin-bioptix-shifts-focus-to-blockchain [Accessed 08 Aug. 2018]

Kharif Olga, 4 Dicembre 2017. CryptoKitties Mania Overwhelms Ethereum Network's Processing. Bloomberg [online]. Disponibile su: https://www.bloomberg.com/news/articles/2017-12-04/cryptokitties-quickly-becomes-most-widely-used-ethereum-app? [Accessed 18 May 2018]

Leising Matthew e Jennifer Surane, 11 Gennaio 2018. MoneyGram Jumps After Saying It'll Test Ripple's Digital Coins. Bloomberg[online]. Disponibile su: https://www.bloomberg.com/news/articles/2018-01-11/ripple-says-moneygram-will-test-its-digital-asset-for-payments [Accessed 02 Jul. 2018]

Maranz Felice, 13 Febbraio 2018. Western Union Says It's Testing Transactions With Ripple. Bloomberg[online]. Disponibile su: https://www.bloomberg.com/news/articles/2018-02-13/western-union-says-it-s-testing-transactions-with-ripple [Accessed 02 Jul. 2018]

Morabito Vincenzo, 2017. Business Innovation Through Blockchain: The B3 Perspective. 1st ed. 2017. Springer Verlag. Pag. 10

North Douglass, 1994. Economic Performance Through Time. The American Economic Review, Vol. 84, No. 3 pp. 359-368

Ou Elanie, 7 Dicembre 2017. No, Bitcoin Won't Boil the Oceans. Bloomberg[online]. Disponibile su: https://www.bloomberg.com/view/articles/2017-12-07/bitcoin-is-greener-than-its-critics-think [Accessed 25 Apr. 2018]

Pedro Franco, 2015. Understanding Bitcoin: Criptography, engineering and economics. 1st ed. 2015. United Kingdom: John Wiley & Sons Ltd. Pag 36-37

Rotman Parker Sarah, 2014. Bitcoin Versus Electronic Money. CGAP (Consultative Group to Assist the Poor) [online]. Disponibile su: http://www.cgap.org/web-publication/bitcoin-versus-electronic-money [Accessed 22 Apr. 2018]

Soldavini Pierangelo, 16 Ottobre 2016. Il contratto si fa smart. Il Sole 24 Ore . Disponibile su: http://nova.ilsole24ore.com/progetti/il-contratto-si-fa-smart/? [Accessed 21 May 2018]

Thompson Patrick, 03 Maggio 2018. How To Diversify Away Risk In A Crypto Portfolio: Correlation And Variance. Conitelegraph [Online]. Disponibile su: https://cointelegraph.com/news/how-to-diversify-away-risk-in-a-crypto-portfolio-correlation-and-variance [Accessed 03 May 2018]

Valsania Marco, 25 Agosto 2016. Big bank unite per creare un proprio bitcoin. Il Sole 24 Ore. Disponibile su: http://www.ilsole24ore.com/art/finanza-e-mercati/2016-08-25/big-bank-unite-creare-proprio-bitcoin-063907.shtml? [Accessed 04 Aug. 2018]

World Food Programme: Building Blocks project. Disponibile su: https://innovation.wfp.org/project/building-blocks [Accessed 26 May 2018]

PUBBLICAZIONI LEGALI

Rapporto sulla stabilità finanziaria, N°1- Aprile 2018, pag n° 11. Disponibile su: http://www.bancaditalia.it/pubblicazioni/rapporto-stabilita/2018-1/RSF-1-2018.pdf [Accessed 22 May 2018]

Risoluzione n° 72/ E Agenzia delle entrate del 2 Settembre 2016 sul: Trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a monete virtuali.

SITOGRAFIA

https://www.spindox.it/

https://slock.it/

https://ripple.com/

https://github.com/DavidJohnstonCEO/DecentralizedApplications/blob/master/README.md